

SO1P1687US0

BEST AVAILABLE COPY



日 本 国 特 許 庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office

出 願 年 月 日

Date of Application:

2000年11月 8日

出 願 番 号

Application Number:

特願2000-340153

出 願 人

Applicant(s):

ソニー株式会社

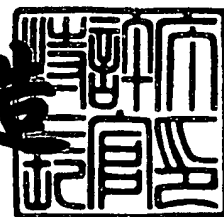
CERTIFIED COPY OF
PRIORITY DOCUMENT

BEST AVAILABLE COPY

2001年10月26日

特 許 庁 長 官
Commissioner,
Japan Patent Office

及 川 耕 造



出 証 番 号 出 証 特 2001-3094899

【書類名】 特許願

【整理番号】 0000571405

【提出日】 平成12年11月 8日

【あて先】 特許庁長官殿

【国際特許分類】 H04L 12/00
H04L 9/00

【発明者】

【住所又は居所】 東京都品川区東五反田1丁目14番10号 株式会社ソニー木原研究所内

【氏名】 大森 睦弘

【特許出願人】

【識別番号】 000002185

【氏名又は名称】 ソニー株式会社

【代表者】 出井 伸之

【代理人】

【識別番号】 100082131

【弁理士】

【氏名又は名称】 稲本 義雄

【電話番号】 03-3369-6479

【手数料の表示】

【予納台帳番号】 032089

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 9708842

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 情報処理装置および方法、記録媒体、並びにサービス提供システム

【特許請求の範囲】

【請求項 1】 第 1 のネットワーク特定情報により特定される、ユーザの個人情報管理する第 1 のサーバとともに、所定のネットワークに接続される第 2 のサーバが、第 2 のネットワーク特定情報により特定される処理を実行することで、所定のサービスの提供を受ける情報処理装置において、

前記第 1 のネットワーク特定情報を記憶する記憶手段と、

前記第 2 のネットワーク特定情報を取得する第 1 の取得手段と、

前記ユーザを認証するために必要な認証データを取得する第 2 の取得手段と、

前記第 1 の取得手段により取得された前記第 2 のネットワーク特定情報により特定される処理が前記第 2 のサーバにより実行されることで、前記サービスの提供を受けることができるように、前記記憶手段に記憶されている前記第 1 のネットワーク特定情報により特定される前記個人情報を管理する前記第 1 のサーバに、前記第 1 のネットワーク特定情報および前記第 2 のネットワーク特定情報を含む制御情報を送信する送信手段と

を備えることを特徴とする情報処理装置。

【請求項 2】 前記第 1 のネットワーク特定情報または前記第 2 のネットワーク特定情報は、URL である

ことを特徴とする請求項 1 に記載の情報処理装置。

【請求項 3】 前記送信手段は、前記情報処理装置に対する、前記ネットワークのアクセスポートとしてのアクセスポート端末が、前記ネットワークに接続されている場合、前記アクセスポート端末を介して、前記制御情報を、前記第 1 のサーバに送信する

ことを特徴とする請求項 1 に記載の情報処理装置。

【請求項 4】 前記送信手段は、指向性のある赤外線、または高周波の電波を利用して、前記制御情報を、前記アクセスポート端末に送信する

ことを特徴とする請求項 3 に記載の情報処理装置。

【請求項 5】 前記第 2 の取得手段は、前記認証データとして、前記ユーザが身に着けている物に組み込まれた認証データ用 IC チップが発生するパスワードを取得する

ことを特徴とする請求項 1 に記載の情報処理装置。

【請求項 6】 前記パスワードは、ワンタイムパスワードである
ことを特徴とする請求項 5 に記載の情報処理装置。

【請求項 7】 前記パスワードは、前記情報処理装置と前記第 1 のサーバとの共通鍵で暗号化されている

ことを特徴とする請求項 5 に記載の情報処理装置。

【請求項 8】 前記パスワードは、前記第 1 のサーバの公開鍵で暗号化されている

ことを特徴とする請求項 5 に記載の情報処理装置。

【請求項 9】 前記第 2 の取得手段は、前記第 1 のサーバからの所定の要求に対して、前記ユーザが身に着けている物に組み込まれた認証データ用 IC チップから適切な応答があったとき、前記認証データ用 IC チップが発生するパスワードを取得する

ことを特徴とする請求項 1 に記載の情報処理装置。

【請求項 10】 前記認証データ用 IC チップが組み込まれた前記ユーザに身に着けられている物は、腕時計、指輪、または前記認証データ用 IC チップに対する防水が施された前記腕時計若しくは前記指輪である

ことを特徴とする請求項 5 に記載の情報処理装置。

【請求項 11】 前記認証データ用 IC チップは、前記情報処理装置からの電磁誘導起電力、光電変換による電力、小型電池からの電力、または前記ユーザの人体からの熱による熱起電力に基づいて動作する

ことを特徴とする請求項 5 に記載の情報処理装置。

【請求項 12】 前記第 2 の取得手段は、前記認証データとして、指紋、声紋、虹彩、または人体の特定部分の血管の造影等を取得する

ことを特徴とする請求項 5 に記載の情報処理装置。

【請求項 13】 前記第 1 の取得手段は、前記第 2 のネットワーク特定情報

を、自分自身が有するマイクロフォンにより取り込まれた前記音声、自分自身が有するイメージセンサにより得られた画像、自分自身が有する前記赤外線センサにより受光された赤外線、または自分自身が有する高周波アンテナにより受信された高周波から取得する

ことを特徴とする請求項 1 に記載の情報処理装置。

【請求項 1 4】 第 1 のネットワーク特定情報により特定される、ユーザの個人情報を管理する第 1 のサーバとともに、所定のネットワークに接続される第 2 のサーバが、第 2 のネットワーク特定情報により特定される処理を実行することで、所定のサービスの提供を受ける情報処理装置の情報処理方法において、

前記第 1 のネットワーク特定情報を記憶する記憶ステップと、

前記第 2 のネットワーク特定情報を取得する第 1 の取得ステップと、

前記ユーザを認証するために必要な認証データを取得する第 2 の取得ステップと、

前記第 1 の取得ステップの処理で取得された前記第 2 のネットワーク特定情報により特定される処理が前記第 2 のサーバにより実行されることで、前記サービスの提供を受けることができるように、前記記憶ステップに記憶されている前記第 1 のネットワーク特定情報により特定される前記個人情報を管理する前記第 1 のサーバに、前記第 1 のネットワーク特定情報および前記第 2 のネットワーク特定情報を含む制御情報を送信する送信ステップと

を含むことを特徴とする情報処理方法。

【請求項 1 5】 第 1 のネットワーク特定情報により特定される、ユーザの個人情報を管理する第 1 のサーバとともに、所定のネットワークに接続される第 2 のサーバが、第 2 のネットワーク特定情報により特定される処理を実行することで、所定のサービスの提供を受ける情報処理装置のプログラムにおいて、

前記第 1 のネットワーク特定情報を記憶する記憶ステップと、

前記第 2 のネットワーク特定情報を取得する第 1 の取得ステップと、

前記ユーザを認証するために必要な認証データを取得する第 2 の取得ステップと、

前記第 1 の取得ステップの処理で取得された前記第 2 のネットワーク特定情報

により特定される処理が前記第 2 のサーバにより実行されることで、前記サービスの提供を受けることができるように、前記記憶ステップに記憶されている前記第 1 のネットワーク特定情報により特定される前記個人情報を管理する前記第 1 のサーバに、前記第 1 のネットワーク特定情報および前記第 2 のネットワーク特定情報を含む制御情報を送信する送信ステップと

を含むことを特徴とするコンピュータが読み取り可能なプログラムが記録されている記録媒体。

【請求項 1 6】 それぞれネットワークを介して接続される、第 1 のネットワーク特定情報を保持する携帯端末、前記第 1 のネットワーク特定情報により特定される、ユーザの個人情報を管理する第 1 のサーバ、および第 2 のネットワーク特定情報により特定される処理を実行する第 2 のサーバからなるサービス提供システムにおいて、

前記携帯端末は、

前記第 1 のネットワーク特定情報を記憶する第 1 の記憶手段と、

前記第 2 のネットワーク特定情報を取得する第 1 の取得手段と、

前記ユーザを認証するために必要な認証データを取得する第 2 の取得手段と

前記第 1 の取得手段により取得された前記第 2 のネットワーク特定情報により特定される処理が前記第 2 のサーバにより実行されることで、所定のサービスの提供を受けることができるように、前記第 1 の記憶手段に記憶されている前記第 1 のネットワーク特定情報により特定される前記個人情報を管理する前記第 1 のサーバに、前記第 1 のネットワーク特定情報および前記第 2 のネットワーク特定情報を含む制御情報を供給する第 1 の供給手段と、

前記第 2 の取得手段により取得された前記認証データを、前記第 1 のサーバに供給する第 2 の供給手段と

を備え、

前記第 1 のサーバは、

前記第 1 のネットワーク特定情報により特定される前記個人情報を管理する第 1 の管理手段と、

前記携帯端末の前記第 1 の供給手段により供給された前記制御情報に含まれる前記第 2 のネットワーク特定情報により特定される処理を実行する前記第 2 のサーバに、前記制御情報および前記個人情報に基づく前記サービスの提供を要求する第 1 の要求手段と、

前記第 2 のサーバからの要求に基づいて、前記携帯端末の前記第 2 の供給手段により供給された前記認証データに基づき前記ユーザを認証する第 1 の認証手段と、

前記第 1 の認証手段による認証結果を、前記第 2 のサーバに供給する第 3 の供給手段と

を備え、

前記第 2 のサーバは、

前記第 2 のネットワーク特定情報により特定される処理を管理する第 2 の管理手段と、

前記第 1 のサーバの第 1 の要求手段による要求があったとき、前記ユーザの認証を前記第 1 のサーバに要求する第 2 の要求手段と、

前記第 1 のサーバの第 3 の供給手段により供給された前記認証結果が、前記ユーザが、前記サービス提供システムの正規のユーザである旨を示しているとき、前記第 2 のネットワーク特定情報により特定される処理を、前記制御情報および前記個人情報に基づいて実行する第 1 の実行手段と

を備えることを特徴とするサービス提供システム。

【請求項 1 7】 前記第 1 のネットワーク特定情報または前記第 2 のネットワーク特定情報は、URL である

ことを特徴とする請求項 1 6 に記載のサービス提供システム。

【請求項 1 8】 前記携帯端末に対する、前記ネットワークのアクセスポートとしてのアクセスポート端末が、前記ネットワークにさらに接続されている場合において、

前記携帯端末の前記第 1 の供給手段または前記第 2 の供給手段は、前記制御情報または前記認証データを、前記アクセスポート端末に供給し、

前記アクセスポート端末は、前記携帯端末の前記第 1 の供給手段または前記第

2 の供給手段から供給された前記制御情報または前記認証データを、前記第 1 のサーバに供給する第 4 の供給手段

を備えることを特徴とする請求項 1 6 に記載のサービス提供システム。

【請求項 1 9】 前記サービス提供システムの使用料金を決済する第 3 のサーバが、前記ネットワークにさらに接続されている場合において、

前記アクセスポート端末は、自分自身が処理した所定の通信量を計測するとともに、その計測結果を、前記第 3 のサーバに供給する第 5 の供給手段をさらに備え、

前記第 3 のサーバは、前記アクセスポート端末の前記第 5 の供給手段から供給された前記計測結果に基づいて、前記サービス提供システムの使用料金を決済する決済手段

を備えることを特徴とする請求項 1 8 に記載のサービス提供システム。

【請求項 2 0】 前記通信量は、前記アクセスポート端末が、前記携帯端末または前記第 1 のサーバに転送したデータ量である

ことを特徴とする請求項 1 9 に記載のサービス提供システム。

【請求項 2 1】 前記携帯端末の、

前記第 1 の記憶手段は、前記第 1 のネットワーク特定情報の公開鍵をさらに記憶し、

前記第 2 の供給手段は、前記第 1 のネットワーク特定情報の公開鍵を、前記アクセスポート端末にさらに供給し、

前記アクセスポート端末の前記第 4 の供給手段は、前記携帯端末の前記第 2 の供給手段により供給された、前記第 1 のネットワーク特定情報の公開鍵で、前記認証データを暗号化し、暗号化された前記認証データを、前記制御情報とともに、前記第 1 のサーバに供給し、

前記第 1 のサーバの、

前記第 1 の管理手段は、前記第 1 のネットワーク特定情報の秘密鍵を個人情報としてさらに管理し、

前記第 1 の認証手段は、前記個人情報に含まれる前記第 1 のネットワーク特定情報の秘密鍵で、前記アクセスポート端末の前記第 4 の供給手段から供給さ

れた前記認証データの暗号化を解凍し、暗号化が解凍された前記認証データに基づいて、前記ユーザを認証する

ことを特徴とする請求項 1 8 に記載のサービス提供システム。

【請求項 2 2】 前記第 1 のサーバの前記第 1 の管理手段は、前記第 1 の認証手段により、前記ユーザが、前記サービス提供システムの正規のユーザであると認証されたとき、前記第 1 のネットワーク特定情報の秘密鍵を変更し、

前記第 1 のサーバは、前記第 1 の管理手段による、前記第 1 のネットワーク特定情報の秘密鍵の変更に対応させて、前記第 1 のネットワーク特定情報の公開鍵を変更するように、前記携帯端末に要求する第 3 の要求手段をさらに備え、

前記携帯端末の前記第 1 の記憶手段は、前記第 1 のサーバの前記第 3 の要求手段による要求に基づいて、前記第 1 のネットワーク特定情報の公開鍵を変更することを特徴とする請求項 2 1 に記載のサービス提供システム。

【請求項 2 3】 前記携帯端末の第 2 の取得手段は、前記ユーザが身に着けた所定の物に組み込まれている認証データ用 IC チップが第 1 のアルゴリズムで発生する、前記認証データとしてのパスワードを取得する

ことを特徴とする請求項 1 6 に記載のサービス提供システム。

【請求項 2 4】 前記パスワードは、ワンタイムパスワードである
ことを特徴とする請求項 2 3 に記載のサービス提供システム。

【請求項 2 5】 前記パスワードは、前記携帯端末と前記第 1 のサーバとの共通鍵で暗号化されている

ことを特徴とする請求項 2 3 に記載のサービス提供システム。

【請求項 2 6】 前記パスワードは、前記第 1 のサーバの公開鍵で暗号化されている

ことを特徴とする請求項 2 3 に記載のサービス提供システム。

【請求項 2 7】 前記携帯端末の第 2 の取得手段は、前記第 1 のサーバからの所定の要求に対して、前記ユーザが身に着けている物に組み込まれた認証データ用 IC チップから適切な応答があったとき、前記認証データ用 IC チップが発生するパスワードを取得する

ことを特徴とする請求項 1 6 に記載のサービス提供システム。

【請求項 2 8】 前記第 1 のサーバの前記第 1 の認証手段は、前記認証データ用 IC チップの前記第 1 のアルゴリズムと同じ第 2 のアルゴリズムで、前記ワンタイムパスワードを発生し、前記携帯端末の前記第 2 の供給手段から供給された、前記認証データとしての前記パスワードと照合することによって、前記ユーザを認証する

ことを特徴とする請求項 2 3 に記載のサービス提供システム。

【請求項 2 9】 前記第 1 のサーバの前記第 1 の認証手段は、前記ユーザが、前記サービス提供システムの正規のユーザであると認証したとき、前記第 2 のアルゴリズムを更新し、

前記第 1 のサーバは、前記第 1 の認証手段による、前記第 2 のアルゴリズムの更新に対応させて、前記認証データ用 IC チップの前記第 1 のアルゴリズムを更新するように、前記携帯端末に要求する第 3 の要求手段をさらに備え、

前記携帯端末は、前記第 1 のサーバの前記第 3 の要求手段による要求に基づいて、前記第 1 のアルゴリズムを更新するように、前記認証データ用 IC チップに要求する第 4 の要求手段

をさらに備えることを特徴とする請求項 2 8 に記載のサービス提供システム。

【請求項 3 0】 前記第 2 のサーバの前記第 1 の実行手段により、前記第 2 のネットワーク特定情報により特定される処理が実行されたとき、所定のサービス情報が、前記携帯端末に供給される場合において、

前記第 1 のサーバの前記第 1 の管理手段は、前記携帯端末の公開鍵をさらに管理し、

前記第 1 のサーバは、前記サービス情報を、前記携帯端末の公開鍵で暗号化し、暗号化された前記サービス情報を、前記携帯端末に供給する第 4 の供給手段をさらに備え、

前記携帯端末の前記第 1 の記憶手段は、自分自身の秘密鍵をさらに記憶し、

前記携帯端末は、前記第 1 のサーバの前記第 4 の供給手段により供給された前記サービス情報の暗号化を、前記自分自身の秘密鍵で解凍する解凍手段

をさらに備えることを特徴とする請求項 1 6 に記載のサービス提供システム。

【請求項 3 1】 前記第 1 のサーバの前記第 1 の管理手段は、前記第 1 の認

証手段により、前記ユーザが、前記サービス提供システムの正規のユーザであると認証したとき、前記携帯端末の公開鍵を変更し、

前記第 1 のサーバは、前記第 1 の管理手段による、前記携帯端末の公開鍵の変更に対応させて、前記携帯端末の秘密鍵を変更するように、前記携帯端末に要求する第 3 の要求手段をさらに備え、

前記携帯端末の前記第 1 の記憶手段は、前記第 1 のサーバの前記第 3 の要求手段による要求に基づいて、前記携帯端末の秘密鍵を変更する

ことを特徴とする請求項 3 0 に記載のサービス提供システム。

【請求項 3 2】 所定のサービス端末がさらに前記ネットワークに接続され、前記第 2 のネットワーク特定情報により特定される処理が精算処理である場合において、

前記携帯端末の、

前記第 1 の取得手段は、前記第 2 のネットワーク特定情報とともに、金額情報を、前記サービス端末から取得し、

前記第 1 の供給手段は、前記精算処理が前記第 2 のサーバにより実行されることで、前記金額情報に示される料金の精算を行うことができるように、前記第 1 のサーバに、前記第 1 のネットワーク特定情報、前記第 2 のネットワーク特定情報、および前記金額情報を含む前記制御情報を供給し、

前記第 1 のサーバの前記第 1 の要求手段は、前記携帯端末の前記第 1 の供給手段により供給された前記制御情報に含まれる前記第 2 のネットワーク特定情報により特定される前記精算処理を実行する前記第 2 のサーバに、前記金額情報および前記個人情報に基づく精算を行うことを要求し、

前記第 2 のサーバの前記第 1 の実行手段は、前記第 1 のサーバの前記第 3 の供給手段により供給された前記認証結果が、前記ユーザが、前記サービス提供システムの正規のユーザである旨を示しているとき、前記精算処理を、前記金額情報および前記個人情報に基づいて実行する

ことを特徴とする請求項 1 6 に記載のサービス提供システム。

【請求項 3 3】 前記携帯端末の、

前記第 1 の取得手段は、支払 ID を、前記サービス端末からさらに取得し、

前記第 1 の供給手段は、前記支払 ID をさらに含む制御情報を、前記第 1 のサーバに供給し、

前記第 1 のサーバの前記第 1 の要求手段は、前記第 2 のサーバに、前記金額情報、前記個人情報、および前記支払 ID に基づく精算を行うことを要求し、

前記第 2 のサーバの前記第 1 の実行手段は、前記第 1 のサーバの前記第 3 の供給手段により供給された前記認証結果が、前記ユーザが、前記サービス提供システムの正規のユーザである旨を示しているとき、前記精算処理を、前記金額情報、前記個人情報、および前記支払 ID に基づいて実行する

ことを特徴とする請求項 3 2 記載のサービス提供システム。

【請求項 3 4】 前記携帯端末に対する、前記ネットワークのアクセスポートとしてのアクセスポート端末が、前記ネットワークにさらに接続されている場合において、

前記携帯端末の前記第 1 の供給手段または前記第 2 の供給手段は、前記制御情報または前記認証データを、前記アクセスポート端末に供給し、

前記アクセスポート端末は、前記携帯端末の前記第 1 の供給手段または前記第 2 の供給手段から供給された前記制御情報または前記認証データを、前記第 1 のサーバに供給する第 4 の供給手段

を備えることを特徴とする請求項 3 2 に記載のサービス提供システム。

【請求項 3 5】 前記第 1 のサーバの第 1 の管理手段は、前記ユーザの特徴情報をさらに管理し、

前記第 1 のサーバは、前記第 2 のサーバからの要求に応じて、前記特徴情報を、前記サービス端末に供給する第 5 の供給手段をさらに備え、

前記サービス端末は、

前記第 1 のサーバの前記第 5 の供給手段により供給された前記特徴情報を利用して、前記ユーザを認証する第 2 の認証手段と、

前記第 2 の認証手段による認証結果を、前記第 2 のサーバに供給する第 5 の供給手段と

をさらに備え、

前記第 2 のサーバの前記第 1 の実行手段は、前記サービス端末の前記第 5 の供

給手段により供給された前記認識結果が、前記ユーザが、前記サービス提供システムの正規のユーザである旨を示しているとき、前記第2のネットワーク特定情報により特定される処理を、前記制御情報および前記個人情報に基づいて実行する

ことを特徴とする請求項34に記載のサービス提供システム。

【請求項36】 前記ユーザの特徴情報は、前記ユーザの顔の部分の画像データであり、

前記サービス端末の前記第2の認証手段による認証は、前記サービス端末の表示部に、前記ユーザの顔の部分の画像データに対応する画像を表示させ、前記サービス端末の管理者が、前記ユーザの実際の顔と、前記画像を照合することで行われる

ことを特徴とする請求項35に記載のサービス提供システム。

【請求項37】 前記第2のサーバは、

前記第1のサーバの前記第3の供給手段により供給された前記認証結果に、所定の有効期限を付して記憶する第2の記憶手段と、

前記第1のサーバの前記第1の要求手段による要求に基づいて、前記第2の記憶手段に記憶されている前記認証結果が有効であるか否かを、前記有効期限に基づいて判定する判定手段と

をさらに備え、

前記第2のサーバの前記第1の実行手段は、前記判定手段により、前記認証結果が有効であると判定されたとき、前記第2のネットワーク特定情報により特定される処理を実行する

ことを特徴とする請求項16に記載のサービス提供システム。

【請求項38】 所定のチケットを購入することで、通過することができる、ゲートの開閉を制御するサービス端末が、前記ネットワークにさらに接続されている場合において、

前記第1のサーバの前記第3の供給手段は、前記認証手段により、前記ユーザが、前記サービス提供システムの正規のユーザであると認識されたとき、前記認証結果として、前記第1のネットワーク特定情報を、前記第2のサーバに供給し

前記第 2 のサーバの、

前記第 2 の記憶手段は、前記第 1 のサーバの前記第 3 の供給手段により供給された前記第 1 のネットワーク特定情報を、前記チケットの発券時に決定された前記有効期限を付して記憶し、

前記判定手段は、前記第 1 のサーバの前記第 1 の要求手段による要求に基づいて、前記第 2 の記憶手段に記憶されている前記第 1 のネットワーク特定情報が有効であるか否かを、前記有効期限に基づいて判定し、

前記第 1 の実行手段は、前記判定手段により、前記第 1 のネットワーク特定情報が有効であると判定されたとき、前記ゲートを開放する処理を実行することを特徴とする請求項 3 7 に記載のサービス提供システム。

【請求項 3 9】 前記第 1 のサーバの、

前記第 1 の管理手段は、前記認証結果を、所定の有効期限を付して管理し、

前記第 1 の認証手段は、前記第 2 のサーバの前記第 2 の要求手段による要求に基づいて、前記認証結果が有効であるか否かを、前記有効期限に基づいて判定し、

前記第 3 の供給手段は、前記認証結果を、前記第 2 のサーバに供給し、
前記第 2 のサーバの、

前記第 2 の要求手段は、所定のタイミングで、前記ユーザの認証を、前記第 1 のサーバに要求し、

前記第 1 の実行手段は、前記第 1 のサーバの前記第 3 の供給手段により供給された前記認証結果が、前記認証結果が有効である旨を示しているとき、前記第 2 のネットワーク特定情報により特定される処理を、前記制御情報および前記個人情報に基づいて実行する

ことを特徴とする請求項 1 6 に記載のサービス提供システム。

【請求項 4 0】 前記サービス提供システムが、それぞれ異なる前記第 2 のネットワーク特定情報により特定される処理を実行する 1 個または複数のサービス処理実行装置をさらに含む場合において、

前記第 1 のサーバの前記第 1 の要求手段は、前記第 2 のサーバおよび前記サー

ビス処理実行装置に、前記制御情報および前記個人情報に基づく前記サービスの提供を要求し、

前記サービス処理実行装置は、それぞれの前記第 2 のネットワーク特定情報により特定される処理を実行する第 2 の実行手段

を備えることを特徴とする請求項 1 6 に記載のサービス提供システム。

【請求項 4 1】 前記サービス処理実行装置の前記第 2 の実行手段は、パーソナルコンピュータを構成する、モニタ、マウス、またはキーボードとしての処理を実行し、

前記第 2 のサーバは、前記パーソナルコンピュータを構成する CPU としての処理を実行する

ことを特徴とする請求項 4 0 に記載のサービス提供システム。

【請求項 4 2】 前記携帯端末は、前記第 1 のネットワーク特定情報を、1 個または複数の前記サービス処理実行装置に供給する第 4 の供給手段

をさらに備え、

前記 1 個または複数のサービス処理実行装置の前記第 2 の実行手段は、前記携帯端末の前記第 4 の供給手段により、前記第 1 のネットワーク特定情報が供給されたときにのみ、前記第 2 のネットワーク特定情報により特定される処理を実行する

ことを特徴とする請求項 4 0 に記載のサービス提供システム。

【請求項 4 3】 1 個の前記サービス処理実行装置の前記第 2 の実行手段が、前記キーボードとしての処理を実行し、前記第 2 のサーバが、文章作成処理を実行している場合において、

前記第 1 のサーバの、

前記第 1 の管理手段は、前記キーボードに対する前記ユーザに対する、文字入力パターンを含む前記個人情報を管理し、

前記第 1 の要求手段は、前記携帯端末の前記第 1 の供給手段により供給された前記制御情報に含まれる前記第 2 のネットワーク特定情報により特定される処理を実行する前記第 2 のサーバに、前記制御情報、および前記文字入力パターンに基づく前記文書作成処理の実行を要求し、

前記第 2 のサーバの前記第 1 の実行手段は、前記制御情報および前記文字入力パターンに基づいて前記文章作成処理を実行する

ことを特徴とする請求項 4 0 に記載のサービス提供システム。

【請求項 4 4】 前記第 2 のサーバの前記第 1 の実行手段により、前記第 2 のネットワーク特定情報により特定される処理が実行された結果、前記携帯端末が所定のサービス情報の提供を受ける場合において、

前記携帯端末は、

前記サービス情報を一時的に記憶する第 2 の記憶手段と、

前記第 2 の記憶手段に記憶されている前記サービス情報のデータ量を監視し

所定のデータ量以上の前記サービス情報が記憶されたとき、ブックマークが付されていない前記サービス情報、または前記ブックマークが付されたホームページとリンクされていない前記サービス情報を、優先的に削除する削除手段とをさらに備えることを特徴とする請求項 1 6 に記載のサービス提供システム。

【請求項 4 5】 前記削除手段は、前記ブックマークに優先順位を設け、必要に応じて、前記優先順位に従って、前記ブックマークに付された前記サービス情報を削除する

ことを特徴とする請求項 4 4 に記載のサービス提供システム。

【請求項 4 6】 前記サービス情報が、前記個人情報である場合、前記第 1 のサーバは、前記個人情報に、前記個人情報が前記携帯端末の前記第 2 の記憶手段に記憶することができないものであることを示すタグを付して、前記携帯端末に供給する第 4 の供給手段

をさらに備えることを特徴とする請求項 4 5 に記載のサービス提供システム。

【請求項 4 7】 前記第 2 のサーバの前記第 1 の実行手段により、前記第 2 のネットワーク特定情報により特定される処理が実行された結果、前記第 1 のサーバが所定のサービス情報の提供を受ける場合において、

前記第 1 のサーバは、

前記サービス情報を一時的に記憶する第 2 の記憶手段と、

前記第 2 の記憶手段に記憶されている前記サービス情報のデータ量を監視し

所定のデータ量以上の前記サービス情報が記憶されたとき、ブックマークが付されていない前記サービス情報、または前記ブックマークが付されたホームページとリンクされていない前記サービス情報を、優先的に削除する削除手段とをさらに備えることを特徴とする請求項 1 6 に記載のサービス提供システム。

【請求項 4 8】 前記削除手段は、前記ブックマークに優先順位を設け、必要に応じて、前記優先順位に従って、前記ブックマークに付された前記サービス情報を削除する

ことを特徴とする請求項 4 7 に記載のサービス提供システム。

【請求項 4 9】 前記第 2 のネットワーク特定情報により特定される処理が、ウェブブラウジングのための処理である場合、前記第 1 のサーバの前記第 1 の管理手段は、一度閲覧したホームページを再度閲覧するのに有効な所定の情報をさらに管理する

ことを特徴とする請求項 1 6 に記載のサービス提供システム。

【請求項 5 0】 それぞれネットワークを介して接続される、第 1 のネットワーク特定情報を保持する携帯端末、前記第 1 のネットワーク特定情報により特定される、ユーザの個人情報を管理する第 1 のサーバ、第 2 のネットワーク特定情報により特定される処理を実行する第 2 のサーバ、前記第 2 のネットワーク特定情報を保持するサービス端末からなるサービス提供システムにおいて、

前記携帯端末は、

前記第 1 のネットワーク特定情報を記憶する記憶手段と、

前記第 2 のネットワーク特定情報およびアクセスパターン検出のためのアクセス情報を、前記サービス端末から取得する第 1 の取得手段と、

前記第 1 の取得手段により取得された前記第 2 のネットワーク特定情報により特定される処理が前記第 2 のサーバにより実行されることで、所定のサービスの提供を受けることができるように、前記記憶手段に記憶されている前記第 1 のネットワーク特定情報により特定される前記個人情報を管理する前記第 1 のサーバに、前記第 1 のネットワーク特定情報、前記第 2 のネットワーク特定情報、および前記アクセス情報を含む制御情報を、前記サービス端末に供給す

る第 1 の供給手段と

を備え、

前記サービス端末は、

前記第 2 のネットワーク特定情報を保持する第 1 の保持手段と、

前記携帯端末の前記第 1 の取得手段による自分自身に対するアクセスから、
前記アクセス情報を取得する第 2 の取得手段と、

前記携帯端末の前記第 1 の取得手段により取得されるように、前記第 2 のネットワーク特定情報および前記アクセス情報を、前記携帯端末に供給する第 2 の供給手段と、

前記携帯端末の前記第 1 の供給手段により供給された前記制御情報を、前記第 1 のサーバに供給する第 3 の供給手段と
を備え、

前記第 1 のサーバは、

前記第 1 のネットワーク特定情報により特定される前記個人情報を管理する第 1 の管理手段と、

前記サービス端末の前記第 2 の供給手段により供給された前記制御情報に含まれる前記第 2 のネットワーク特定情報により特定される処理を実行する前記第 2 のサーバに、前記制御情報、前記個人情報、および前記アクセス情報に基づく前記サービスの提供を要求する第 1 の要求手段と
を備え、

前記第 2 のサーバは、

前記第 2 のネットワーク特定情報により特定される処理を管理する第 2 の管理手段と、

前記第 1 のサーバの前記第 1 の要求手段による要求に基づいて、前記第 2 のネットワーク特定情報により特定される前記処理を、前記制御情報、前記個人情報、および前記アクセス情報に基づいて実行する実行手段と
を備えることを特徴とするサービス提供システム。

【請求項 5 1】 第 1 の前記サービス端末が、第 1 の場所に設けられ、第 2 の前記サービス端末が、第 2 の場所に設けられ、前記携帯端末の前記第 1 の取得

手段は、前記第 1 のサービス端末に先にアクセスし、その後、前記第 2 のサービス端末にアクセスする場合において、

前記アクセス情報は、アクセスされた時刻を含み、

前記第 2 のサーバの実行手段は、前記第 1 のサービス端末の前記第 1 の取得手段により取得された前記アクセス情報に含まれる前記時刻と、前記第 2 のサービス端末の前記第 1 の取得手段により取得された前記アクセス情報に含まれる時刻との差分を算出するとともに、その算出結果が、所定の時間以上であるか否かを判定し、前記時間以上であると判定した場合、前記第 2 のネットワーク特定情報により特定される処理を実行する

ことを特徴とする請求項 5 0 に記載のサービス提供システム。

【請求項 5 2】 前記第 1 の場所および前記第 2 の場所は、遊園地の通路の所定の場所または有料道路の入口若しくは出口付近の所定の場所である

ことを特徴とする請求項 5 1 に記載のサービス提供システム。

【請求項 5 3】 前記第 1 の場所が、前記有料道路の入口付近の所定の場所であり、前記第 2 の場所が、前記有料道路の出口付近の所定の場所である場合において、

前記第 2 のサービス端末は、

通過する車両を撮像する撮像手段と、

前記撮像手段による撮像結果から、前記車両の前記車両番号を取得する第 3 の取得手段と

を備え、

前記第 2 のサービス端末の前記第 3 の供給手段は、前記第 3 の取得手段により取得された前記車両番号を、前記第 1 のサーバにさらに供給し、

前記第 1 のサーバの前記第 1 の要求手段は、前記第 2 のサービス端末の前記第 3 の供給手段により供給された前記制御情報に含まれる前記第 2 のネットワーク特定情報により特定される処理を実行する前記第 2 のサーバに、前記制御情報、前記個人情報、前記アクセス情報、および前記第 2 のサービス端末の前記第 2 の取得手段により取得された前記車両番号に基づく前記サービスの提供を要求し、

前記第 2 のサーバは、前記ユーザの車両の車両番号を予め保持する第 2 の保持

手段をさらに備え、

前記第 2 のサーバの前記実行手段は、前記第 2 のサービス端末の前記第 2 の取得手段により取得された前記車両番号が、前記第 2 の保持手段により保持されている前記車両番号と一致するか否かを判定し、一致すると判定した場合、前記有料道路の通行料金の精算処理を、前記制御情報および前記個人情報に基づいて実行する

ことを特徴とする請求項 5 2 に記載のサービス提供システム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、情報処理装置、情報処理方法、および記録媒体、並びにサービス提供システムに関し、特に、例えば、ユーザが利用する端末を紛失しても、安全に利用することができるようにした情報処理装置、情報処理方法、および記録媒体、並びにサービス提供システムに関する。

【0002】

【従来の技術】

ユーザが携帯端末を操作し、所定のネットワークに接続されているサーバと通信を行うことで、そのサーバから、所定のサービスの提要を受けることができるサービス提供システムが存在する。

【0003】

【発明が解決しようとする課題】

しかしながら、通常、この携帯端末に、サービス提供システムを利用するために必要なユーザ ID やユーザ認証のためのパスワードなどの個人情報が記憶されているようになされている。すなわち、例えば、携帯端末を紛失した場合、それらの個人情報が悪用されてしまう課題があった。

【0004】

また、個人情報を送受信する場合、その漏洩を防止するために、携帯端末において暗号化がされる場合もあるが、通常の携帯端末の機能では、高度な暗号化を行うことができない。すなわち、個人情報が解読され、漏洩する課題があった。

【 0 0 0 5 】

さらに、携帯端末として携帯電話を利用することもできるが、携帯電話の使用は、例えば、心臓ペースメーカ等の医療用の精密機器への影響を考慮して、場所によって制限されている。すなわち、このシステムの利用が制限されてしまう課題があった。

【 0 0 0 6 】

以上のように、従来のサービス提供システムでは、その利用に多くの制限が課される課題があった。

【 0 0 0 7 】

本発明はこのような状況に鑑みてなされたものであり、ユーザに多くの制限を課すことなく、サービス提供システムを利用することができるようにするものである。

【 0 0 0 8 】

【課題を解決するための手段】

本発明の情報処理装置は、第1のネットワーク特定情報を記憶する記憶手段と、第2のネットワーク特定情報を取得する第1の取得手段と、ユーザを認証するために必要な認証データを取得する第2の取得手段と、第1の取得手段により取得された第2のネットワーク特定情報により特定される処理が第2のサーバにより実行されることで、サービスの提供を受けることができるように、記憶手段に記憶されている第1のネットワーク特定情報により特定される個人情報を管理する第1のサーバに、第1のネットワーク特定情報および第2のネットワーク特定情報を含む制御情報を送信する送信手段とを備えることを特徴とする。

【 0 0 0 9 】

第1のネットワーク特定情報または第2のネットワーク特定情報は、URLとすることができる。

【 0 0 1 0 】

送信手段は、情報処理装置に対する、ネットワークのアクセスポートとしてのアクセスポート端末が、ネットワークに接続されている場合、アクセスポート端末を介して、制御情報を、第1のサーバに送信することができる。

【 0 0 1 1 】

送信手段は、指向性のある赤外線、または高周波の電波を利用して、制御情報を、アクセスポート端末に送信することができる。

【 0 0 1 2 】

第 2 の取得手段は、認証データとして、ユーザが身に着けている物に組み込まれた認証データ用 I C チップが発生するパスワードを取得することができる。

【 0 0 1 3 】

パスワードは、ワンタイムパスワードとすることができる。

【 0 0 1 4 】

パスワードは、情報処理装置と第 1 のサーバとの共通鍵で暗号化されているものとすることができる。

【 0 0 1 5 】

パスワードは、第 1 のサーバの公開鍵で暗号化されているものとすることができる。

【 0 0 1 6 】

第 2 の取得手段は、第 1 のサーバからの所定の要求に対して、ユーザが身に着けている物に組み込まれた認証データ用 I C チップから適切な応答があったとき、認証データ用 I C チップが発生するパスワードを取得することができる。

【 0 0 1 7 】

認証データ用 I C チップが組み込まれたユーザに身に着けられている物は、腕時計、指輪、または認証データ用 I C チップに対する防水が施された腕時計若しくは指輪とすることができる。

【 0 0 1 8 】

認証データ用 I C チップは、情報処理装置からの電磁誘導起電力、光電変換による電力、小型電池からの電力、またはユーザの人体からの熱による熱起電力に基づいて動作することができる。

【 0 0 1 9 】

第 2 の取得手段は、認証データとして、指紋、声紋、虹彩、または人体の特定部分の血管の造影等を取得することができる。

【0020】

第1の取得手段は、第2のネットワーク特定情報を、自分自身が有するマイクロフォンにより取り込まれた音声、自分自身が有するイメージセンサにより得られた画像、自分自身が有する赤外線センサにより受光された赤外線、または自分自身が有する高周波アンテナにより受信された高周波から取得することができる。

【0021】

本発明の情報処理方法は、第1のネットワーク特定情報を記憶する記憶ステップと、第2のネットワーク特定情報を取得する第1の取得ステップと、ユーザを認証するために必要な認証データを取得する第2の取得ステップと、第1の取得ステップの処理で取得された第2のネットワーク特定情報により特定される処理が第2のサーバにより実行されることで、サービスの提供を受けることができるように、記憶ステップに記憶されている第1のネットワーク特定情報により特定される個人情報を管理する第1のサーバに、第1のネットワーク特定情報および第2のネットワーク特定情報を含む制御情報を送信する送信ステップとを含むことを特徴とする。

【0022】

本発明の記録媒体のプログラムは、第1のネットワーク特定情報を記憶する記憶ステップと、第2のネットワーク特定情報を取得する第1の取得ステップと、ユーザを認証するために必要な認証データを取得する第2の取得ステップと、第1の取得ステップの処理で取得された第2のネットワーク特定情報により特定される処理が第2のサーバにより実行されることで、サービスの提供を受けることができるように、記憶ステップに記憶されている第1のネットワーク特定情報により特定される個人情報を管理する第1のサーバに、第1のネットワーク特定情報および第2のネットワーク特定情報を含む制御情報を送信する送信ステップとを含むことを特徴とする。

【0023】

本発明の情報処理装置および方法、並びに記録媒体のプログラムにおいては、第1のネットワーク特定情報が記憶され、第2のネットワーク特定情報が取得さ

れ、ユーザを認証するために必要な認証データが取得され、取得された第2のネットワーク特定情報により特定される処理が第2のサーバにより実行されることで、サービスの提供を受けることができるように、記憶されている第1のネットワーク特定情報により特定される個人情報を管理する第1のサーバに、第1のネットワーク特定情報および第2のネットワーク特定情報を含む制御情報が送信される。

【 0 0 2 4 】

本発明の第1のサービス提供システムは、携帯端末が、第1のネットワーク特定情報を記憶する第1の記憶手段と、第2のネットワーク特定情報を取得する第1の取得手段と、ユーザを認証するために必要な認証データを取得する第2の取得手段と、第1の取得手段により取得された第2のネットワーク特定情報により特定される処理が第2のサーバにより実行されることで、所定のサービスの提供を受けることができるように、第1の記憶手段に記憶されている第1のネットワーク特定情報により特定される個人情報を管理する第1のサーバに、第1のネットワーク特定情報および第2のネットワーク特定情報を含む制御情報を供給する第1の供給手段と、第2の取得手段により取得された認証データを、第1のサーバに供給する第2の供給手段とを備え、第1のサーバが、第1のネットワーク特定情報により特定される個人情報を管理する第1の管理手段と、携帯端末の第1の供給手段により供給された制御情報に含まれる第2のネットワーク特定情報により特定される処理を実行する第2のサーバに、制御情報および個人情報に基づくサービスの提供を要求する第1の要求手段と、第2のサーバからの要求に基づいて、携帯端末の第2の供給手段により供給された認証データに基づきユーザを認証する第1の認証手段と、第1の認証手段による認証結果を、第2のサーバに供給する第3の供給手段とを備え、第2のサーバが、第2のネットワーク特定情報により特定される処理を管理する第2の管理手段と、第1のサーバの第1の要求手段による要求があったとき、ユーザの認証を第1のサーバに要求する第2の要求手段と、第1のサーバの第3の供給手段により供給された認証結果が、ユーザが、第1のサービス提供システムの正規のユーザである旨を示しているとき、第2のネットワーク特定情報により特定される処理を、制御情報および個人情報

に基づいて実行する第1の実行手段とを備えることを特徴とする。

【0025】

第1のネットワーク特定情報または第2のネットワーク特定情報は、URLとすることができる。

【0026】

携帯端末に対する、ネットワークのアクセスポートとしてのアクセスポート端末が、ネットワークにさらに接続されている場合において、携帯端末の第1の供給手段または第2の供給手段は、制御情報または認証データを、アクセスポート端末に供給し、アクセスポート端末は、携帯端末の第1の供給手段または第2の供給手段から供給された制御情報または認証データを、第1のサーバに供給する第4の供給手段を設けることができる。

【0027】

第1のサービス提供システムの使用料金を決済する第3のサーバが、ネットワークにさらに接続されている場合において、アクセスポート端末には、自分自身が処理した所定の通信量を計測するとともに、その計測結果を、第3のサーバに供給する第5の供給手段をさらに設け、第3のサーバには、アクセスポート端末の第5の供給手段から供給された計測結果に基づいて、第1のサービス提供システムの使用料金を決済する決済手段を設けることができる。

【0028】

通信量は、アクセスポート端末が、携帯端末または第1のサーバに転送したデータ量とすることができる。

【0029】

携帯端末の、第1の記憶手段は、第1のネットワーク特定情報の公開鍵をさらに記憶し、第2の供給手段は、第1のネットワーク特定情報の公開鍵を、アクセスポート端末にさらに供給し、アクセスポート端末の第4の供給手段は、携帯端末の第2の供給手段により供給された、第1のネットワーク特定情報の公開鍵で、認証データを暗号化し、暗号化された認証データを、制御情報とともに、第1のサーバに供給し、第1のサーバの、第1の管理手段は、第1のネットワーク特定情報の秘密鍵を個人情報としてさらに管理し、第1の認証手段は、個人情報に

含まれる第1のネットワーク特定情報の秘密鍵で、アクセスポート端末の第4の供給手段から供給された認証データの暗号化を解凍し、暗号化が解凍された認証データに基づいて、ユーザを認証することができる。

【0030】

第1のサーバの第1の管理手段は、第1の認証手段により、ユーザが、第1のサービス提供システムの正規のユーザであると認証されたとき、第1のネットワーク特定情報の秘密鍵を変更し、第1のサーバには、第1の管理手段による、第1のネットワーク特定情報の秘密鍵の変更に対応させて、第1のネットワーク特定情報の公開鍵を変更するように、携帯端末に要求する第3の要求手段をさらに設け、携帯端末の第1の記憶手段は、第1のサーバの第3の要求手段による要求に基づいて、第1のネットワーク特定情報の公開鍵を変更することができる。

【0031】

携帯端末の第2の取得手段は、ユーザが身に着けた所定の物に組み込まれている認証データ用ICチップが第1のアルゴリズムで発生する、認証データとしてのパスワードを取得することができる。

【0032】

パスワードは、ワンタイムパスワードとすることができる。

【0033】

パスワードは、携帯端末と第1のサーバとの共通鍵で暗号化されているものとすることができる。

【0034】

パスワードは、第1のサーバの公開鍵で暗号化されているものとすることができる。

【0035】

携帯端末の第2の取得手段は、第1のサーバからの所定の要求に対して、ユーザが身に着けている物に組み込まれた認証データ用ICチップから適切な応答があったとき、認証データ用ICチップが発生するパスワードを取得することができる。

【0036】

第 1 のサーバの第 1 の認証手段は、認証データ用 IC チップの第 1 のアルゴリズムと同じ第 2 のアルゴリズムで、ワンタイムパスワードを発生し、携帯端末の第 2 の供給手段から供給された、認証データとしてのパスワードと照合することによって、ユーザを認証することができる。

【 0 0 3 7 】

第 1 のサーバの第 1 の認証手段は、ユーザが、第 1 のサービス提供システムの正規のユーザであると認証したとき、第 2 のアルゴリズムを更新し、第 1 のサーバには、第 1 の認証手段による、第 2 のアルゴリズムの更新に対応させて、認証データ用 IC チップの第 1 のアルゴリズムを更新するように、携帯端末に要求する第 3 の要求手段をさらに設け、携帯端末には、第 1 のサーバの第 3 の要求手段による要求に基づいて、第 1 のアルゴリズムを更新するように、認証データ用 IC チップに要求する第 4 の要求手段をさらに設けることができる。

【 0 0 3 8 】

第 2 のサーバの第 1 の実行手段により、第 2 のネットワーク特定情報により特定される処理が実行されたとき、所定のサービス情報が、携帯端末に供給される場合において、第 1 のサーバの第 1 の管理手段は、携帯端末の公開鍵をさらに管理し、第 1 のサーバには、サービス情報を、携帯端末の公開鍵で暗号化し、暗号化されたサービス情報を、携帯端末に供給する第 4 の供給手段をさらに設け、携帯端末の第 1 の記憶手段は、自分自身の秘密鍵をさらに記憶し、携帯端末は、第 1 のサーバの第 4 の供給手段により供給されたサービス情報の暗号化を、自分自身の秘密鍵で解凍する解凍手段をさらに設けることができる。

【 0 0 3 9 】

第 1 のサーバの第 1 の管理手段は、第 1 の認証手段により、ユーザが、第 1 のサービス提供システムの正規のユーザであると認証したとき、携帯端末の公開鍵を変更し、第 1 のサーバには、第 1 の管理手段による、携帯端末の公開鍵の変更に対応させて、携帯端末の秘密鍵を変更するように、携帯端末に要求する第 3 の要求手段をさらに設け、携帯端末の第 1 の記憶手段は、第 1 のサーバの第 3 の要求手段による要求に基づいて、携帯端末の秘密鍵を変更することができる。

【 0 0 4 0 】

所定のサービス端末がさらにネットワークに接続され、第2のネットワーク特定情報により特定される処理が精算処理である場合において、携帯端末の、第1の取得手段は、第2のネットワーク特定情報とともに、金額情報を、サービス端末から取得し、第1の供給手段は、精算処理が第2のサーバにより実行されることで、金額情報に示される料金の精算を行うことができるように、第1のサーバに、第1のネットワーク特定情報、第2のネットワーク特定情報、および金額情報を含む制御情報を供給し、第1のサーバの第1の要求手段は、携帯端末の第1の供給手段により供給された制御情報に含まれる第2のネットワーク特定情報により特定される精算処理を実行する第2のサーバに、金額情報および個人情報に基づく精算を行うことを要求し、第2のサーバの第1の実行手段は、第1のサーバの第3の供給手段により供給された認証結果が、ユーザが、第1のサービス提供システムの正規のユーザである旨を示しているとき、精算処理を、金額情報および個人情報に基づいて実行することができる。

【 0 0 4 1 】

携帯端末の、第1の取得手段は、支払IDを、サービス端末からさらに取得し、第1の供給手段は、支払IDをさらに含む制御情報を、第1のサーバに供給し、第1のサーバの第1の要求手段は、第2のサーバに、金額情報、個人情報、および支払IDに基づく精算を行うことを要求し、第2のサーバの第1の実行手段は、第1のサーバの第3の供給手段により供給された認証結果が、ユーザが、第1のサービス提供システムの正規のユーザである旨を示しているとき、精算処理を、金額情報、個人情報、および支払IDに基づいて実行することができる。

【 0 0 4 2 】

携帯端末に対する、ネットワークのアクセスポートとしてのアクセスポート端末が、ネットワークにさらに接続されている場合において、携帯端末の第1の供給手段または第2の供給手段は、制御情報または認証データを、アクセスポート端末に供給し、アクセスポート端末には、携帯端末の第1の供給手段または第2の供給手段から供給された制御情報または認証データを、第1のサーバに供給する第4の供給手段を設けることができる。

【 0 0 4 3 】

第1のサーバの第1の管理手段は、ユーザの特徴情報をさらに管理し、第1のサーバには、第2のサーバからの要求に応じて、特徴情報を、サービス端末に供給する第5の供給手段をさらに設け、サービス端末には、第1のサーバの第5の供給手段により供給された特徴情報を利用して、ユーザを認証する第2の認証手段と、第2の認証手段による認証結果を、第2のサーバに供給する第5の供給手段とをさらに設け、第2のサーバの第1の実行手段は、サービス端末の第5の供給手段により供給された認証結果が、ユーザが、第1のサービス提供システムの正規のユーザである旨を示しているとき、第2のネットワーク特定情報により特定される処理を、制御情報および個人情報に基づいて実行することができる。

【0044】

ユーザの特徴情報は、ユーザの顔の部分の画像データであり、サービス端末の第2の認証手段による認証は、サービス端末の表示部に、ユーザの顔の部分の画像データに対応する画像を表示させ、サービス端末の管理者が、ユーザの実際の顔と、画像を照合することで行われるようにすることができる。

【0045】

第2のサーバには、第1のサーバの第3の供給手段により供給された認証結果に、所定の有効期限を付して記憶する第2の記憶手段と、第1のサーバの第1の要求手段による要求に基づいて、第2の記憶手段に記憶されている認証結果が有効であるか否かを、有効期限に基づいて判定する判定手段とをさらに設け、第2のサーバの第1の実行手段は、判定手段により、認証結果が有効であると判定されたとき、第2のネットワーク特定情報により特定される処理を実行することができる。

【0046】

所定のチケットを購入することで、通過することができる、ゲートの開閉を制御するサービス端末が、ネットワークにさらに接続されている場合において、第1のサーバの第3の供給手段は、認証手段により、ユーザが、第1のサービス提供システムの正規のユーザであると認識されたとき、認証結果として、第1のネットワーク特定情報を、第2のサーバに供給し、第2のサーバの、第2の記憶手段は、第1のサーバの第3の供給手段により供給された第1のネットワーク特定

情報を、チケットの発券時に決定された有効期限を付して記憶し、判定手段は、第1のサーバの第1の要求手段による要求に基づいて、第2の記憶手段に記憶されている第1のネットワーク特定情報が有効であるか否かを、有効期限に基づいて判定し、第1の実行手段は、判定手段により、第1のネットワーク特定情報が有効であると判定されたとき、ゲートを開放する処理を実行することができる。

【 0 0 4 7 】

第1のサーバの、第1の管理手段は、認証結果を、所定の有効期限を付して管理し、第1の認証手段は、第2のサーバの第2の要求手段による要求に基づいて、認証結果が有効であるか否かを、有効期限に基づいて判定し、第3の供給手段は、認証結果を、第2のサーバに供給し、第2のサーバの、第2の要求手段は、所定のタイミングで、ユーザの認証を、第1のサーバに要求し、第1の実行手段は、第1のサーバの第3の供給手段により供給された認証結果が、認証結果が有効である旨を示しているとき、第2のネットワーク特定情報により特定される処理を、制御情報および個人情報に基づいて実行することができる。

【 0 0 4 8 】

第1のサービス提供システムが、それぞれ異なる第2のネットワーク特定情報により特定される処理を実行する1個または複数のサービス処理実行装置をさらに含む場合において、第1のサーバの第1の要求手段は、第2のサーバおよびサービス処理実行装置に、制御情報および個人情報に基づくサービスの提供を要求し、サービス処理実行装置には、それぞれの第2のネットワーク特定情報により特定される処理を実行する第2の実行手段を設けることができる。

【 0 0 4 9 】

サービス処理実行装置の第2の実行手段は、パーソナルコンピュータを構成する、モニタ、マウス、またはキーボードとしての処理を実行し、第2のサーバは、パーソナルコンピュータを構成するCPUとしての処理を実行することができる。携帯端末には、第1のネットワーク特定情報を、1個または複数のサービス処理実行装置に供給する第4の供給手段をさらに設け、1個または複数のサービス処理実行装置の第2の実行手段は、携帯端末の第4の供給手段により、第1のネットワーク特定情報が供給されたときにのみ、第2のネットワーク特定情報に

より特定される処理を実行することができる。

【0050】

1個のサービス処理実行装置の第2の実行手段が、キーボードとしての処理を実行し、第2のサーバが、文章作成処理を実行している場合において、第1のサーバの、第1の管理手段は、キーボードに対するユーザに対する、文字入力パターンを含む個人情報を管理し、第1の要求手段は、携帯端末の第1の供給手段により供給された制御情報に含まれる第2のネットワーク特定情報により特定される処理を実行する第2のサーバに、制御情報、および文字入力パターンに基づく文書作成処理の実行を要求し、第2のサーバの第1の実行手段は、制御情報および文字入力パターンに基づいて文章作成処理を実行することができる。

【0051】

第2のサーバの第1の実行手段により、第2のネットワーク特定情報により特定される処理が実行された結果、携帯端末が所定のサービス情報の提供を受ける場合において、携帯端末には、サービス情報を一時的に記憶する第2の記憶手段と、第2の記憶手段に記憶されているサービス情報のデータ量を監視し、所定のデータ量以上のサービス情報が記憶されたとき、ブックマークが付されていないサービス情報、またはブックマークが付されたホームページとリンクされていないサービス情報を、優先的に削除する削除手段とをさらに設けることができる。

【0052】

削除手段は、ブックマークに優先順位を設け、必要に応じて、優先順位に従って、ブックマークに付されたサービス情報を削除することができる。

【0053】

サービス情報が、個人情報である場合、第1のサーバには、個人情報に、個人情報に携帯端末の第2の記憶手段に記憶することができないものであることを示すタグを付して、携帯端末に供給する第4の供給手段をさらに設けることができる。

【0054】

第2のサーバの第1の実行手段により、第2のネットワーク特定情報により特定される処理が実行された結果、第1のサーバが所定のサービス情報の提供を受

ける場合において、第1のサーバには、サービス情報を一時的に記憶する第2の記憶手段と、第2の記憶手段に記憶されているサービス情報のデータ量を監視し、所定のデータ量以上のサービス情報が記憶されたとき、ブックマークが付されていないサービス情報、またはブックマークが付されたホームページとリンクされていないサービス情報を、優先的に削除する削除手段とをさらに設けることができる。

【0055】

削除手段は、ブックマークに優先順位を設け、必要に応じて、優先順位に従って、ブックマークに付されたサービス情報を削除することができる。

【0056】

第2のネットワーク特定情報により特定される処理が、ウェブブラウジングのための処理である場合、第1のサーバの第1の管理手段は、一度閲覧したホームページを再度閲覧するのに有効な所定の情報をさらに管理することができる。

【0057】

本発明の第1のサービス提供システムにおいては、携帯端末で、第1のネットワーク特定情報が記憶され、第2のネットワーク特定情報が取得され、ユーザを認証するために必要な認証データが取得され、取得された第2のネットワーク特定情報により特定される処理が第2のサーバにより実行されることで、所定のサービスの提供を受けることができるように、記憶されている第1のネットワーク特定情報により特定される個人情報を管理する第1のサーバに、第1のネットワーク特定情報および第2のネットワーク特定情報を含む制御情報が供給され、取得された認証データが、第1のサーバに供給され、第1のサーバで、第1のネットワーク特定情報により特定される個人情報が管理され、供給された制御情報に含まれる第2のネットワーク特定情報により特定される処理を実行する第2のサーバに、制御情報および個人情報に基づくサービスの提供が要求され、第2のサーバからの要求に基づいて、供給された認証データに基づきユーザが認証され、認証結果が、第2のサーバに供給され、第2のサーバで、第2のネットワーク特定情報により特定される処理が管理され、要求があったとき、ユーザの認証が第1のサーバに要求され、供給された認証結果が、ユーザが、サービス提供システ

ムの正規のユーザである旨を示しているとき、第2のネットワーク特定情報により特定される処理が、制御情報および個人情報に基づいて実行される。

【 0 0 5 8 】

本発明の第2のサービス提供システムは、携帯端末が、第1のネットワーク特定情報を記憶する記憶手段と、第2のネットワーク特定情報およびアクセスパターン検出のためのアクセス情報を、サービス端末から取得する第1の取得手段と、第1の取得手段により取得された第2のネットワーク特定情報により特定される処理が第2のサーバにより実行されることで、所定のサービスの提供を受けることができるように、記憶手段に記憶されている第1のネットワーク特定情報により特定される個人情報を管理する第1のサーバに、第1のネットワーク特定情報、第2のネットワーク特定情報、およびアクセス情報を含む制御情報を、サービス端末に供給する第1の供給手段とを備え、サービス端末が、第2のネットワーク特定情報を保持する第1の保持手段と、携帯端末の第1の取得手段による自分自身に対するアクセスから、アクセス情報を取得する第2の取得手段と、携帯端末の第1の取得手段により取得されるように、第2のネットワーク特定情報およびアクセス情報を、携帯端末に供給する第2の供給手段と、携帯端末の第1の供給手段により、制御情報が供給された制御情報を、第1のサーバに供給する第3の供給手段とを備え、第1のサーバが、第1のネットワーク特定情報により特定される個人情報を管理する第1の管理手段と、サービス端末の第2の供給手段により供給された制御情報に含まれる第2のネットワーク特定情報により特定される処理を実行する第2のサーバに、制御情報、個人情報、およびアクセス情報に基づくサービスの提供を要求する第1の要求手段とを備え、第2のサーバが、第2のネットワーク特定情報により特定される処理を管理する第2の管理手段と、第1のサーバの第1の要求手段による要求に基づいて、第2のネットワーク特定情報により特定される処理を、制御情報、個人情報、およびアクセス情報に基づいて実行する実行手段とを備えることを特徴とする。

【 0 0 5 9 】

第1のサービス端末が、第1の場所に設けられ、第2のサービス端末が、第2の場所に設けられ、携帯端末の第1の取得手段は、第1のサービス端末に先にア

クセスし、その後、第2のサービス端末にアクセスする場合において、アクセス情報は、アクセスされた時刻を含み、第2のサーバの実行手段は、第1のサービス端末の第1の取得手段により取得されたアクセス情報に含まれる時刻と、第2のサービス端末の第1の取得手段により取得されたアクセス情報に含まれる時刻との差分を算出するとともに、その算出結果が、所定の時間以上であるか否かを判定し、時間以上であると判定した場合、第2のネットワーク特定情報により特定される処理を実行することができる。

【0060】

第1の場所および第2の場所は、遊園地の通路の所定の場所または有料道路の入口若しくは出口付近の所定の場所とすることができる。

【0061】

第1の場所が、有料道路の入口付近の所定の場所であり、第2の場所が、有料道路の出口付近の所定の場所である場合において、第2のサービス端末には、通過する車両を撮像する撮像手段と、撮像手段による撮像結果から、車両の車両番号を取得する第3の取得手段とを設け、第2のサービス端末の第3の供給手段は、第3の取得手段により取得された車両番号を、第1のサーバにさらに供給し、第1のサーバの第1の要求手段は、第2のサービス端末の第3の供給手段により供給された制御情報に含まれる第2のネットワーク特定情報により特定される処理を実行する第2のサーバに、制御情報、個人情報、アクセス情報、および第2のサービス端末の第2の取得手段により取得された車両番号に基づくサービスの提供を要求し、第2のサーバには、ユーザの車両の車両番号を予め保持する第2の保持手段をさらに設け、第2のサーバの実行手段は、第2のサービス端末の第2の取得手段により取得された車両番号が、第2の保持手段により保持されている車両番号と一致するか否かを判定し、一致すると判定した場合、有料道路の通行料金の精算処理を、制御情報および個人情報に基づいて実行することができる。

【0062】

本発明の第2のサービス提供システムにおいては、携帯端末で、第1のネットワーク特定情報が記憶され、第2のネットワーク特定情報およびアクセスパター

ン検出のためのアクセス情報が、サービス端末から取得され、取得された第2のネットワーク特定情報により特定される処理が第2のサーバにより実行されることで、所定のサービスの提供を受けることができるように、記憶されている第1のネットワーク特定情報により特定される個人情報を管理する第1のサーバに、第1のネットワーク特定情報、第2のネットワーク特定情報、およびアクセス情報を含む制御情報が、サービス端末に供給され、サービス端末で、第2のネットワーク特定情報が保持され、自分自身に対するアクセスから、アクセス情報が取得され、取得されるように、第2のネットワーク特定情報およびアクセス情報が、携帯端末に供給され、供給された制御情報が、第1のサーバに供給され、第1のサーバで、第1のネットワーク特定情報により特定される個人情報が管理され、供給された制御情報に含まれる第2のネットワーク特定情報により特定される処理を実行する第2のサーバに、制御情報、個人情報、およびアクセス情報に基づくサービスの提供が要求され、第2のサーバで、第2のネットワーク特定情報により特定される処理が管理され、要求に基づいて、第2のネットワーク特定情報により特定される処理が、制御情報、個人情報、およびアクセス情報に基づいて実行される。

【0063】

【発明の実施の形態】

図1は、本発明を適用したサービス提供システムの利用例を示している。この場合、ユーザAは、サービス提供システムを利用して、料金の精算を行う。

【0064】

腕時計1は、ユーザAに身に着けられている腕時計であるが、この腕時計1には、携帯端末2と通信し、携帯端末2からの要求に応じて、一回の処理に限りパスワードとして利用される文字列等（以下、ワンタイムパスワードと称する）を、所定のアルゴリズムで発生し、携帯端末2に送信する機能を有するICチップ（以下、認証データ用ICチップと称する）（図2）が組み込まれている。

【0065】

なお、腕時計1の他、指輪などに認証データ用ICチップを組み込ませてもできる。すなわち、このように、身に着けておくことができる物に、認証

データ用 ICチップを組み込ませておくことで、このシステムの利用がより容易になる。

【0066】

また、腕時計 1 に防水性を持たせ、いつでも（例えば、お風呂に入っているときにでも）身に付けておくことができるようにすることもできる。

【0067】

携帯端末 2 は、携帯に便利な小型の装置で、ユーザ A による操作に応じて、精算装置 3-1 を介してネットワーク 4 に接続し、例えば、個人サーバ 5 と通信する。携帯端末 2 は、個人サーバ 5 に記憶されているユーザ A の個人情報（例えば、URL（以下、URL 1 と称する）を記憶しており、その URL 1 を、精算装置 3-1 に送信し、精算装置 3-1 が、それに基づく通信を行うことで、個人サーバ 5 との通信が可能となる。

【0068】

なお、ここで URL は、インターネット上のホームページの他、テキストデータ、処理プログラムなどを含む、ネットワーク 4 上に存在する資源を特定することができるものを意味する。

【0069】

精算装置 3-1 は、ユーザ（この例の場合、ユーザ A）が購入する商品の合計値を算出する装置、いわゆるレジであるが、この例の場合、無線で携帯端末 2 と通信することができるとともに、ネットワーク 4 を介して、個人サーバ 5 やサービスサーバ 6-1 とも通信することができる。すなわち、精算装置 3-1 は、携帯端末 2 に対するネットワークアクセスポートとしての役割を果たす。なお、明細書中の各図において、携帯端末 2 に対するネットワークアクセスポートの役割を有する装置には、NAP（ネットワークアクセスポートの略）が付されている。

【0070】

個人サーバ 5 は、URL 1 により特定される、ユーザ A の個人データを管理するサーバであり、ネットワーク 4 を介して、精算装置 3-1 やサービスサーバ 6-1 と通信する。

【 0 0 7 1 】

サービスサーバ 6-1 は、所定の URL（以下、URL 2 と称する）により特定される処理をサーバである。サービスサーバ 6-1 が、その処理を、ネットワーク 4 を介して、精算装置 3-1 や個人サーバ 5 と通信して実行する。これにより、ユーザ A は、各種サービスの提供を受けることができる。

【 0 0 7 2 】

図 2 は、腕時計 1 に組み込まれた認証データ用 IC チップの構成例を示している。CPU 11 は、システムバス 13 を介して接続されるメインメモリ 12 に記憶されているプログラム（例えば、ワンタイムパスワード生成プログラム）を実行し、ワンタイムパスワード等を生成する。

【 0 0 7 3 】

通信部 14 は、無線で携帯端末 2 と通信し、例えば、携帯端末 2 からの認証データ発生要求を受信して、CPU 11 に供給したり、CPU 11 により生成されたワンタイムパスワード等を、携帯端末 2 に送信する。

【 0 0 7 4 】

なお、通信部 14 は、人体を媒体として携帯端末 2 と通信することができるようにすることができる。この場合、例えば、携帯端末 2 がユーザ A の手で直接保持されると、ユーザ A の体を媒体として、腕時計 1（認証データ用 IC チップ）と携帯端末 2 の通信が可能となる。

【 0 0 7 5 】

電源供給部 15 は、各部に電源を供給する。なお、電源供給部 15 を、小型の電池の他、太陽電池で構成し、太陽光から光電変換で電源電力を得るようにすることもできる。また、電源供給部 15 は、電磁誘導起電力、また人体からの熱による熱起電力を、電源電力とすることもできる。

【 0 0 7 6 】

図 3 は、携帯端末 2 の構成例を示している。CPU 21 は、メインメモリ 22 に記憶されているプログラムに従って、各種の処理を実行する。

【 0 0 7 7 】

メインメモリ 22 は、各種プログラムを記憶しているとともに、URL 1（ユ

ーザAの個人情報(を特定するもの)を記憶している。なお、メインメモリ12は、携帯端末2の電源が切られてもその記憶が保持されるSRAMで構成され、いわゆるバッテリーバックアップされている。また、メインメモリ22は、高速動作可能なSRAMと、記憶保持用のフラッシュメモリ等の組み合わせで構成することもできる。

【0078】

入力部23は、CPU21に所定の指令を入力するときユーザにより適宜操作される。表示部24は、例えば、LCD等により構成され、所定の文字、図形、または画像を表示する。出力部25は、スピーカ等で構成され、音声信号を出力する。

【0079】

通信部26は、赤外線通信や、ブルートゥースなどのようにミリ波帯、13.5MHz、または20MHz等の電波を利用して、精算装置3-1(ネットワークアクセスポート)と通信する。すなわち、携帯端末2と精算装置3-1の間では、いわゆる短距離通信が行われるので、ここでの通信により、例えば、心臓ペースメーカー等の精密装置が誤動作するようなことはない。従って、携帯端末2と精算装置3-1の通信を、場所の制限を受けずに行うことができる(場所の制限を受けずに、このシステムを利用することができる)。

【0080】

通信部27は、腕時計1に組み込まれている認証データ用ICチップ(通信部14)と無線で通信する。なお、通信部27は、人体を媒体として認証データ用ICチップと通信することもできる。

【0081】

インターフェース28は、入力部23乃至通信部27とCPU21との間に配置され、インターフェース処理を行う。

【0082】

図4は、精算装置3-1の構成例を示している。CPU31は、ROM32に記憶されているプログラムに従って、各種の処理を実行する。RAM33には、CPU31が各種の処理を実行する上において必要なデータなどが適宜記憶され

る。

【0083】

入力部34は、CPU31に所定の指令を入力するとき適宜操作される。表示部35は、例えば、LCD等により構成され、所定の文字、図形、または画像を表示する。ハードディスク36は、所定のデータ（例えば、URL2）を記憶し、必要に応じて、これを再生する。

【0084】

通信部37は、ネットワーク4に接続されており、それを介して、個人サーバ5やサービスサーバ6-1と通信する。

【0085】

通信部38は、赤外線通信や、ブルートゥースなどのようにミリ波帯、13.5MHz、または20MHzの電波を利用して、携帯端末2と通信する。

【0086】

インターフェース39は、入力部34乃至通信部38とCPU31との間に配置され、インタフェース処理を行う。

【0087】

図5は、個人サーバ5の構成例を示してる。CPU41は、ROM42に記憶されているプログラムに従って、各種の処理を実行する。RAM43には、CPU41が各種の処理を実行する上において必要なデータなどが適宜記憶される。

【0088】

なお、ROM42には、腕時計1（認証データ用ICチップのメインメモリ12）に記憶されているワンタイムパスワード等を生成するプログラムと同様のアルゴリズムでワンタイムパスワード等を生成するプログラムが記憶されている。すなわち、CPU41は、通信部47、ネットワーク4、精算装置3-1、および携帯端末2を介して、腕時計1からのワンタイムパスワード等を受信した場合、そのプログラムを実行し、自分自身でもワンタイムパスワード等を生成する。そしてCPU41は、受信したワンタイムパスワード等と生成したワンタイムパスワード等を照合して、ユーザ認証を行う。

【0089】

入力部44は、CPU41に所定の指令を入力するとき適宜操作される。表示部45は、例えば、LCD等により構成され、所定の文字、図形、または画像を表示する。

【0090】

ハードディスク46は、所定のデータ（例えば、このサービス提供システムに登録された正規のユーザ（ユーザAなど）の氏名、住所、取引銀行の口座番号、ユーザの顔部分の画像データ（以下、顔写真データと称する）などの個人情報を記憶し、これを、必要に応じて再生する。

【0091】

通信部47は、ネットワーク4に接続されており、ネットワーク4を介して、精算装置3-1やサービスサーバ6-1と通信する。

【0092】

インターフェース48は、入力部44乃至通信部47とCPU41との間に配置され、インタフェース処理を行う。

【0093】

サービスサーバ6-1の構成は、基本的に個人サーバ5の場合と同様であるので、その図示および説明は省略するが、そのROMまたはハードディスクには、URL2で特定される処理を実行するためのプログラムが格納されている。

【0094】

次に、精算処理の手順を、図6のフローチャートを参照して説明する。

【0095】

ステップS1において、精算装置3-1は、URL2、金額を示す情報（以下、購入金額と称する）、および支払IDを、携帯端末2に送信する。携帯端末2は、それを受信する。

【0096】

このとき、ユーザAは、購入する商品を、精算装置3-1の付近に設けられた台に運ぶ。店員は、ユーザAにより運ばれた商品の購入金額（合計金額）を、精算装置3-1の入力部34を操作して、算出した後、所定の操作を、精算装置3-1に対して行う。これにより、精算装置3-1は、その操作に対応して、上述

したようなデータを、携帯端末2に送信する。なお、このとき、ユーザA（携帯端末2）は、携帯端末2と精算装置3-1との短距離通信が可能となる程度に、精算装置3-1に近づいている。

【0097】

次に、ステップS2において、携帯端末2は、ステップS1で受信したURL2、購入金額、および支払IDを、精算装置3-1およびネットワーク4を介して、個人サーバ5に送信するとともに、URL2により特定される処理を実行するサービスサーバ6-1との通信を、個人サーバ5に対して要求する。なお、携帯端末2と個人サーバ5との通信は、携帯端末2が、URL1を、精算装置3-1に送信し、精算装置3-1が、それに基づく通信を行うことで可能となる。これにより、個人サーバ5は、携帯端末2から送信されたデータを受信するとともに、その要求を認識する。

【0098】

例えば、このとき、携帯端末2のCPU21は、表示部24を制御して、ステップS1で受信した情報を表示させる。ユーザAは、表示部24に表示された情報を確認すると、入力部23に対して所定の操作を行う。これにより、携帯端末2は、その操作に対応して、ステップS1で受信した情報を、個人サーバ5に送信する。

【0099】

ステップS3において、個人サーバ5は、ステップS2で認識した要求に基づいて、サービスサーバ6-1に対して、接続を要求する。サービスサーバ6-1は、その要求に応答する。これにより、個人サーバ5とサービスサーバ6-1との通信が確立される。

【0100】

次に、ステップS4において、個人サーバ5は、ステップS2で受信した支払IDと購入金額を、サービスサーバ6-1に送信し、サービスサーバ6-1は、それを受信する。

【0101】

ステップS5において、サービスサーバ6-1は、個人サーバ5に対して、ユ

ーザ認証を要求する。個人サーバ5は、その要求を認識する。

【0102】

次に、ステップS6において、顔写真データによるユーザ認証処理が行われる。ここでの処理の詳細は、図7のフローチャートに示されている。

【0103】

ステップS21において、個人サーバ5は、ユーザAの個人情報として記憶している顔写真データを、精算装置3-1に送信する。精算装置3-1は、それを受信する。次に、ステップS22において、精算装置3-1は、顔写真データに対応する画像を表示部35に表示する。

【0104】

ステップS23において、精算装置3-1は、顔写真によるユーザ認証結果を認識する。具体的には、店員は、精算装置3-1の表示部35に表示された顔の画像から、ユーザA本人であるか否かを確認する、すなわち、このシステムに正規に登録されたユーザであるか否かを確認する。そして店員は、その確認結果に応じた操作を、精算装置3-1の入力部34に対して行う。これにより、精算装置3-1は、顔写真によるユーザ認証結果を認識する。

【0105】

次に、ステップS24において、精算装置3-1は、ステップS23で認識したユーザ認証結果を、個人サーバ5とサービスサーバ6-1に送信する。個人サーバ5とサービスサーバ6-1は、それを受信する。なお、ここでは、ユーザAは、正規のユーザであると認証されたものとして、以下の説明を進める。

【0106】

その後、処理は終了し、図6のステップS7に進む。

【0107】

ステップS6で、精算装置3-1から供給された認証結果が、ユーザAが、このシステムの正規のユーザである旨を示しているとき、ステップS7において、認証データによるユーザ認証が行われる。ここでの処理は、図8のフローチャートに示されている。

【0108】

ステップS31において、個人サーバ5は、認証データの提供を、ネットワーク4および精算装置3-1を介して、携帯端末2に要求する。携帯端末2は、その要求を認識する。なお、個人サーバ5と携帯端末2との通信は、常に、ネットワーク4および精算装置3-1を介して行われるので、以下において、個人サーバ5と携帯端末2の通信について記述する場合、「ネットワーク4および精算装置3-1を介して」の文言を、適宜省略する。

【0109】

次に、ステップS32において、携帯端末2は、ステップS31で認識した要求に基づいて、認証データとしてのワンタイムパスワードを、腕時計1から取得する。具体的には、携帯端末2のCPU21は、はじめに、表示部24を制御して、認証データの提供が要求されていることを示すメッセージを表示させる。これにより、ユーザAは、腕時計1を携帯端末2に近づける。（または携帯端末2を手で直接保持する）。その結果、腕時計1（認証データ用ICチップ）と携帯端末2との通信が可能となるので、携帯端末2は、認証データの発生を、認証データ用ICチップに対し要求し、認証データ用ICチップは、その要求に応じてワンタイムパスワードを発生し、携帯端末2に送信する。携帯端末2は、腕時計1からのワンタイムパスワードを受信する。このようにして、携帯端末2は、認証データとしてのワンタイムパスワードを取得する。

【0110】

ステップS33において、携帯端末2は、ステップS32で取得した認証データを、個人サーバ5に送信する。個人サーバ5は、それを受信する。

【0111】

次に、ステップS34において、個人サーバ5は、自分自身でワンタイムパスワードを生成して、ステップS33で受信した認証データと照合し、ユーザ認証を行う。具体的には、上述したように、個人サーバ5のCPU41は、ROM42に記憶されている、認証データ用ICチップが実行するワンタイムパスワード生成プログラムと同様のアルゴリズムでワンタイムパスワードを生成して、受信したワンタイムパスワードと照合する。両者が同じであれば、正規のユーザであると認証される。

【0112】

ステップS35において、個人サーバ5は、ユーザ認証の結果を、サービスサーバ6-1に送信する。サービスサーバ6-1は、それを受信する。

【0113】

なお、ここで、ユーザ認証が成立した場合（この例の場合、ユーザAが正規のユーザであると認証された場合）、個人サーバ5は、ワンタイムパスワードの生成アルゴリズムの更新を行うとともに、その更新に関する情報を、携帯端末2を介して、腕時計1（認証データ用ICチップ）にも送信する。認証データ用ICチップは、それを受信する。これにより、認証データ用ICチップは、個人サーバ5が行った更新に対応させて、自分自身のワンタイムパスワードの生成アルゴリズムを更新する。

【0114】

このように、ユーザ認証が成立したとき、認証データ発生ICチップと個人サーバ5（認証される側と認証する側）のワンタイムパスワードの生成アルゴリズムを更新することで、本システムの不正利用を防止することができる。例えば、ワンタイムパスワードのアルゴリズムが更新されているので、認証データ発生ICチップ自体が複製されても、それが発生するワンタイムパスワードでは、ユーザの認証を得ることができない。

【0115】

その後、処理は終了し、図6のステップS8に進む。なお、ここでは、認証データによるユーザ認証により、ユーザAが正規のユーザであると認証されたものとして、以下の説明を進める。

【0116】

ユーザAが、正規のユーザであると認証されると、ステップS8において、支払処理が行われる。具体的には、サービスサーバ6-1は、料金の振り込み先を、個人サーバ5に通知する。

【0117】

個人サーバ5は、通知された振り込み先のサーバA（図示せず）に対して、所定の振り込み処理を行い、振り込みが完了すると、その旨を、サービスサーバ6

ー１に送信する。なお、このとき個人サーバ５は、例えば、支払ＩＤを添付して電子マネー等をサーバＡに送信し、サーバＡでは、その支払ＩＤを利用して、決済することもできる。なお、ここでは、購入金額に対する支払が完了したものととして、以下の説明を進める。

【０１１８】

購入金額に対する支払が完了すると、ステップＳ９において、サービスサーバ６－１は、ステップＳ４で受信した支払ＩＤを、精算装置３－１に送信する（戻す）。精算装置３－１は、それを受信する。

【０１１９】

ステップＳ１０において、精算装置３－１は、支払処理の完了を認識する。具体的には、精算装置３－１のＣＰＵ３１は、表示部３５を制御して、ステップＳ９で受信した支払ＩＤを表示させる。これにより、店員は、購入金額に対する支払が完了したことを確認し、所定の操作を精算装置３－１の入力部３４に対して行う。これにより、精算装置３－１は、支払処理の完了を認識する。

【０１２０】

その後、処理は終了する。このようにして、購入金額に対する精算が行われる。

【０１２１】

このように、ユーザＡの個人情報は、個人サーバ５に記憶され、携帯端末２には記憶されていないので、例えば、携帯端末２を紛失しても、個人情報が第３者に渡り、悪用されることがない。

【０１２２】

また、携帯端末２とネットワークアクセスポート（精算装置３）との通信は、いわゆる短距離通信であり、心臓ペースメーカー等の精密機器の動作に影響を与えないので、ユーザは、いつでも、携帯端末２で精算装置３と通信を行い、このシステムを利用することができる。

【０１２３】

なお、以上においては、ネットワークアクセスポートとしての精算装置３が設けられている場合を例としてが、携帯端末２が個人サーバ５等と直接通信するこ

とができるようにすることもできる。

【0124】

また、以上においては、ステップS6での顔写真によるユーザ認証、およびステップS7での認証データによるユーザ認証のそれぞれを行うようにしたが、例えば、いずれか一方のユーザ認証だけを行うようにすることもできる。

【0125】

また、以上においては、認証データとして、腕時計1が発生するワンタイムパスワードを利用する場合を例として説明したが、携帯端末2と個人サーバ5との共通鍵で暗号化されたパスワード、または個人サーバ5の公開鍵で暗号化されたパスワードを認証データとすることもできる。さらに、認証データとして、ユーザの指紋、声紋、虹彩、または特定部分の血管の造影等を利用することができる。また、携帯端末2は、個人サーバ5からの要求に応じて、認証用ICチップから適切な応答があったとき、認証用ICチップから、認証データを取得するようにすることができる。

【0126】

図9は、指紋および声紋を認証データとして採取することができる携帯端末2の構成例を示している。すなわち、この携帯端末2には、図3の携帯端末2に、指紋を採取するための指紋採取センサ51と、音声を取り込むマイクロフォン52がさらに設けられている。

【0127】

指紋採取センサ51は、ユーザAが指先の内側（腹）を押し当てることのできるように取り付けられており、指の腹が押し当てられたとき、その指紋データを採取し、CPU21に出力する。またはマイクロフォン52は、ユーザAの音声を取り込みCPU21に出力する。

【0128】

CPU21は、指紋採取センサ51からの指紋データ、またはマイクロフォン52からの音声データを解析し、その特徴データを認証データとして取得する。

【0129】

なお、認証データとしての指紋や声紋の特徴データは、その個人を特定するデ

ータとして重要であるので、指紋や声紋を認証データとして利用する場合、例えば、図8のステップS33の処理で、認証データを、個人サーバ5に送信するとき、暗号化する必要がある。

【0130】

この場合、携帯端末2は、URL1の公開鍵を保持しており、取得した認証データ（指紋又は声紋等の特徴データ）を、そのURL1の公開鍵とともに、精算装置3-1に送信する。精算装置3-1は、それらを受信する。なお、携帯端末2と精算装置3-1の通信は、短距離通信であるので、送信データが改竄される可能性は少ないことから、この例の場合、携帯端末2と精算装置3-1との通信では、認証データは、暗号化されない。ただし、携帯端末2が自身が暗号化することもできる。

【0131】

精算装置3-1は、受信したURL1の公開鍵で、認証データを暗号化し、個人サーバ5に送信する。個人サーバ5は、それを受信する。

【0132】

個人サーバ5は、この場合、URL1の秘密鍵を保持しており、それを利用して、精算装置3-1からの認証データの暗号化を解凍する。

【0133】

個人サーバ5はまた、この場合、ユーザAの指紋や声紋等の特徴データを認証データとして予め（ユーザAの登録時に）記憶しており、図8のステップS34の処理で、暗号化を解凍して得られた認証データと、記憶している認証データとを照合し、ユーザAを認証する。

【0134】

このように、認証データの暗号化が必要な場合、ネットワークアクセスポートとしての精算装置3-1で暗号化するようにしたので、携帯端末2で暗号化を行う場合に比べ、より強固な暗号化を行うことができる。通常、携帯端末2は、小型である必要など、設計上の制限から、強固な暗号化を行うプログラムを実装することができない。

【0135】

また、図8のステップS35で、ワンタイムパスワードの生成アルゴリズムを更新する際に、携帯端末2が保持するURL1の公開鍵と、個人サーバ5が保持するURL1の秘密鍵を、それぞれ対応させて変更することができる。このように、鍵自身を変更することで、より強固な暗号化が可能となる。

【0136】

また、個人サーバ5から、所定の情報を暗号化して、携帯端末2に送信したい場合、個人サーバ5は、携帯端末2の公開鍵を、ユーザAの個人情報として保持し、その公開鍵で、情報を暗号化して、携帯端末2に送信する。携帯端末2は、自分の秘密鍵で、個人サーバ5からの情報の暗号化を解凍する。この場合、ユーザ認証結果に応じて、それぞれの鍵を変更することができる。

【0137】

また、図6の例における、ステップS8での支払処理は、銀行の口座に預けられているお金（現金）による支払を想定しているが、いわゆる商品券を利用する支払を行うこともできる。なお、ここでの商品券とは、それを利用することができる店舗の公開鍵で暗号化された、そこで購入することができる金額を示すデータ（商品券データ）を意味し、例えば、ユーザAが持っている商品券は、個人サーバ5（ハードディスク46）に、ユーザAの個人情報として記憶されている。

【0138】

商品券を利用した精算処理の手順を、図10のフローチャートを参照して説明する。

【0139】

ステップS40乃至ステップS46、およびステップS48、S49においては、図6のステップS1乃至ステップS7、およびステップS9、S10の場合と同様の処理が行われるので、その説明は省略する。

【0140】

ステップS47において、商品券による支払処理が行われる。ここでの処理の詳細は、図11のフローチャートに示されている。

【0141】

ステップS51において、個人サーバ5は、サービスサーバ6-1の公開鍵で

暗号化された商品券データを、サービスサーバ 6-1 に送信する。サービスサーバ 6-1 は、それを受信する。

【0142】

次に、ステップ S 5 2 において、サービスサーバ 6-1 は、自分の秘密鍵で、ステップ S 5 1 で受信した商品券データを解凍する。この場合、サービスサーバ 6-1 は、自分の秘密鍵および公開鍵を予め保持している。

【0143】

ステップ S 5 3 において、サービスサーバ 6-1 は、商品券データに示される購入可能金額から、ステップ S 4 3 で受信した購入金額を減算する。

【0144】

次に、ステップ S 5 4 において、サービスサーバ 6-1 は、その減算結果を、個人サーバ 5 の公開鍵で暗号化して、商品券データを生成（更新）し、個人サーバ 5 に送信する。個人サーバ 5 は、それを受信する。

【0145】

ステップ S 5 5 において、個人サーバ 5 は、ステップ S 5 4 で受信した商品券データを、ユーザ A の個人情報として記憶する。

【0146】

その後、処理は終了し、図 9 のステップ S 4 8 に進む。このようにして、商品券による支払が行われる。

【0147】

また、図 6 の例では、ユーザ A が購入する商品を、精算装置 3-1（レジ）まで持っていき、そして精算装置 3-1 で算出された購入金額分の料金を支払う場合を例として説明したが、次に、例えば、大きくて、精算装置 3 まで運ぶことができない商品を購入する場合について説明する。

【0148】

図 1 2 は、この場合に利用される携帯端末 2 の構成例が示されている。なお図中、図 3 における場合と対応する部分については、同一の符号を付してあり、以下では、その説明は、適宜省略する。

【0149】

すなわち、この携帯端末 2 には、図 3 の携帯端末 2 に、イメージセンサ 6 1 がさらに設けられている。

【0150】

イメージセンサ 6 1 は、この例の場合商品に付されている URL 2（例えば、商品のタグに付されている URL 2）を、画像データとして取得するセンサーである。CPU 2 1 は、イメージセンサ 6 1 により取得された画像データから、URL 2 を認識する。

【0151】

次に、この場合の精算処理の手順について、図 1 3 のフローチャートを参照して説明する。なお、この場合、URL 2 が付された商品の近くにネットワークアクセスポート（図示せず）が設定されているものとする。

【0152】

ステップ S 6 1 において、携帯端末 2（CPU 2 1）は、イメージセンサ 6 1 により得られた画像データから、商品に付された URL 2 を取得する。

【0153】

次に、ステップ S 6 2 において、携帯端末 2 は、ステップ S 6 1 で取得した URL 2 および商品購入を示す信号を、図示せぬネットワークアクセスポートおよびネットワーク 4 を介して、個人サーバ 5 に送信するとともに、URL 2 を管理するサービスサーバ 6 - 1 との通信を要求する。

【0154】

なお、ステップ S 6 1 またはステップ S 6 2 での携帯端末 2 の動作は、ユーザ A による携帯端末 2 に対する所定の動作に対応して行われる。また、このとき、ユーザ A（携帯端末 2）は、携帯端末 2 とネットワークアクセスポートとの短距離通信が可能となる程度に、ネットワークアクセスポートに近づいているものとする。

【0155】

ステップ S 6 3 において、個人サーバ 5 とサービスサーバ 6 - 1 の通信が確立されると、ステップ S 6 4 において、個人サーバ 5 は、URL 2 により指定される商品の購入を示す信号を、サービスサーバ 6 - 1 に送信する。サービスサーバ

6-1 は、それを受信する。

【0156】

ステップ S 6 5 において、サービスサーバ 6-1 は、個人サーバ 5 に対して、ユーザ認証を要求する。個人サーバ 5 は、その要求を認識する。

【0157】

ステップ S 6 6 において、認証データによるユーザ認証が行われる。ここでの処理は、図 6 のステップ S 7 での処理と同様にして行われるので、その説明は省略する。

【0158】

ステップ S 6 6 の処理で、ユーザ A が正規のユーザであると認証されると、ステップ S 6 7 において、サービスサーバ 6-1 は、URL 2 で示される商品の商品情報（例えば、価格情報や商品の紹介情報）を、個人サーバ 5 に送信する。個人サーバ 5 は、それを受信し、そして携帯端末 2 に送信する。携帯端末 2 は、それを受信する。

【0159】

ステップ S 6 8 において、携帯端末 2 は、商品が購入されるか否かを認識する。具体的には、携帯端末 2 の CPU 2 1 は、ステップ S 6 7 で受信した商品情報を、表示部 2 4 に表示させる。ユーザ A は、表示部 2 4 に表示された商品情報に基づいて、その商品を購入するか否かを判断し、その判断結果に応じた操作を、入力部 2 3 に対して行う。これにより、CPU 2 1 は、商品が購入されるか否かを認識する。

【0160】

ユーザ A により、商品購入のための操作が携帯端末 2 の入力部 2 3 に対して行われると、ステップ S 6 9 において、支払処理が行われる。ここでの処理は、図 6 のステップ S 8 での処理と同様であるので、その説明は省略する。

【0161】

なお、例えば、オークション等のように、商品の価格が短い時間内で変動する場合、ステップ S 6 7, 6 8 での処理が繰り返し実行され、ユーザは、随時変化する商品価格を参考にして、その商品の購入を決定することができる。またこの

とき、ユーザAは、携帯端末2の入力部23を操作し、希望価格を入力して、そのオークションに参加することができる。

【0162】

また、図13の例では、イメージセンサ61により取得された画像データから、URL2を取得する場合を例として説明したが、商品に、URL2を示すバーコード（2次元バーコードを含む）が付されている場合、携帯端末2は、バーコードリーダを備え、それでURL2を読み取ることができる。

【0163】

また、URL2が、例えば、その商品の宣伝用の音声に、間欠的に、聞こえない帯域に含まれている場合、携帯端末2は、マイクロフォン52（図9）で、その音声を取り込み、URL2を抽出するようにすることもできる。さらに、URL2が、赤外線で出力されている場合、携帯端末2は、赤外線センサを備え、その赤外線センサにより受光された赤外線から、URL2を抽出したり、URL2が、高周波で所定の送信装置から出力されている場合、携帯端末2は、高周波アンテナを備え、高周波アンテナにより受信された高周波から、URL2を抽出する。

【0164】

また、図13の例では、商品情報が携帯端末2の表示部24に表示される場合を例として説明したが、より大きな画面で表示した方がよい場合等では、図14に示すように、その商品の近くに設けられている、ネットワークアクセスポートとしてのモニタ3-2に、それを表示させることができる。なお、本明細書においては、携帯端末2に対するネットワークアクセスポートとしての機能を有する装置には、“3-”の符号を付してあり、その構成は、精算装置3-1の構成（図4）と基本的に同様である。

【0165】

この場合、基本的には、図13のフローチャートの場合と同様の処理が行われるが、ステップS62に相当する処理で、携帯端末2は、個人サーバ5に、URL2および商品購入を示す信号とともに、モニタ3-2のURL（URL3）を送信する。すなわち、この処理に先立って、ユーザは、見えるように示されてい

る（例えば、モニタ 3-2 に付されている）モニタ 3-2 の URL 3 を確認し、それを、携帯端末 2 の入力部 23 に入力する。

【0166】

これにより、ステップ S 67 に相当する処理で、サービスサーバ 6-1 は、商品情報等を、モニタ 3-2 に送信する。モニタ 3-2 は、それを受信し、表示する。

【0167】

また、このような利用によれば、例えば、サービスサーバ 6-1 が、コンテンツ（楽曲または映像のデータ）を配信する場合、ユーザ A は、コンテンツを購入し、それを自分自身の再生装置（例えば、オーディオ装置やモニタ）に送信させることで、それを見たり聞いたりすることができる。また、再生装置ではなく、個人サーバ 5 に送信させて、そこに記憶させておくことで、ユーザ A は、後からそれを利用することができる。

【0168】

また、サービスサーバ 6-1 が、コンテンツとして楽曲データを提供する場合、1つの宣伝方法として、この楽曲を流すとき（例えば、店内放送や、ラジオ放送で流すとき）、その中にそのコンテンツの URL 2 を含ませておけば、ユーザ A は、それを聴いて気に入れば、携帯端末 2 を操作し、マイクロフォン（マイクロファン 52）からその楽曲を読み取り、URL 2 を取得することで、そのコンテンツを、再生装置や個人サーバ 5 に供給させることができる。

【0169】

また、図 13 の例では、サービスサーバ 6-1 が保持している商品情報をモニタ 3-2 に表示させる場合を例として説明したが、モニタ 3-2 がその情報を保持しているようにすることもできる。

【0170】

また、図 13 の例では、1つの商品の URL 2 を取得し、それについての支払処理を説明したが、ユーザ A は、興味のある複数の商品（実際購入するかはこの時点ではわからない商品）の URL 2（商品によってそれぞれ異なる URL）を取得して、随時その商品情報の提供を受け、後から、その商品情報を参照して、

最終的に購入する商品を決定することもできる。

【0171】

この場合、提供を受けた商品情報を、個人サーバ5が記憶（キャッシュ）し、携帯端末2から要求があった場合、個人サーバ5は、要求された商品情報を、携帯端末2に送信するようにする。このようにすることで、個人サーバ5が記憶している情報について、サービスサーバ6-1に再度アクセスする必要がなくなるので、必要な情報を迅速に閲覧することができ、また通信コスト等を節約することができる。また、例えば、携帯端末2が、個人サーバ5を介して、サービスサーバ6-1に対するウェブブラウジング等を行い、所定のページを閲覧した場合、個人サーバ5が、このときの操作情報をキャッシュしておき、それを、再度そのページを閲覧する際に利用するようにできる。これにより、迅速にそのページにたどり着くことができる。

【0172】

なお、個人サーバ5の他、携帯端末2もデータをキャッシュすることもできる。しかしながら、この場合、個人情報にキャッシュされると、携帯端末2を紛失したとき、その情報が第3者に漏洩することもあり得るので、個人サーバ5は、個人情報を、携帯端末2に送信する際に、その個人情報に、そのキャッシュを許可しない旨を示すタグを付して送信する。このようにすることで、個人サーバ5から送信された個人情報は、携帯端末2でキャッシュされず、携帯端末2が例えば紛失しても、個人情報が、第3者に渡ることを防止することができる。

【0173】

また、個人サーバ5が記憶する情報量には制限があり、その制限を超える場合、記憶している情報を消去する必要がある。このとき、個人サーバ5は、ブックマーク等に登録されていないもの、またはブックマーク等に登録されたページからのリンクに成っていないデータから優先的に消去する。またさらに情報の消去が必要な場合、個人サーバ5は、ブックマークの中で優先順位を設け、その低いものから消去する。

【0174】

図15は、本発明を適用したサービス提供システムの他の利用例を示している

。この場合、ユーザ A は、ブラウジング装置および携帯端末 2 のネットワークアクセスポートとしてのパーソナルコンピュータ 3-3 を利用して、ショッピングサーバ 6-2 に対するネットショッピングを行う。なお、本明細書においては、サービスを提供するサーバには、“6-” の符号を付してあり、その構成は、個人サーバ 5 の構成（図 5）と基本的に同様である。

【0175】

ネットショッピングを行う場合の処理手順は、図 16 のフローチャートに示されている。

【0176】

ステップ S 8 1 において、パーソナルコンピュータ 3-3 は、ネットワーク 4 を介して、ショッピングサーバ 6-2 にアクセスする。ステップ S 8 2 において、パーソナルコンピュータ 3-3 は、購入される商品を認識し、ステップ S 8 3 において、その URL（URL 2）を、携帯端末 2 に送信する。携帯端末 2 は、それを受信する。なお、このとき、ユーザ A（携帯端末 2）は、携帯端末 2 とパーソナルコンピュータ 3-3 との短距離通信が可能となる程度に、パーソナルコンピュータ 3-3 に近づいているものとする。

【0177】

ステップ S 8 1 乃至ステップ S 8 3 でのパーソナルコンピュータ 3-3 の動作は、ユーザ A による、パーソナルコンピュータ 3-3 の、例えば、キーボード等に対する操作に基づいて実行される。

【0178】

次に、ステップ S 8 4 において、携帯端末 2 は、個人サーバ 5 に、ステップ S 8 3 で受信した URL 2 を、パーソナルコンピュータ 3-3 およびネットワーク 4 を介して送信するとともに、URL 2 を管理するショッピングサーバ 6-2 との通信を要求する。個人サーバ 5 は、URL 2 を受信するとともに、その要求を認識する。

【0179】

ステップ S 8 5 で、個人サーバ 5 とショッピングサーバ 6-2 との通信が確立されると、ステップ S 8 6 において、個人サーバ 5 は、URL 2 を、ショッピン

グサーバ6-2に送信し、ショッピングサーバ6-2は、それを受信する。

【0180】

次に、ステップS87において、ショッピングサーバ6-2は、個人サーバ5に対して、ユーザ認証を要求する。個人サーバ5は、その要求の認識する。

【0181】

ステップS88において、認証データによるユーザ認証が行われるが、ここでの処理は、図6のステップS7における処理と同様であるので、その説明は省略する。

【0182】

ステップS88で、ユーザAが、正規のユーザであると認証されると、ステップS89において、支払処理が行われる。ここでの処理は、基本的には、図6のステップS8における処理と同様であるが、URL2で示される商品の金額情報等が、ショッピングサーバ6-2から個人サーバ5に送信され、個人サーバ5は、その額に応じた振り込み処理を行う。

【0183】

ステップS89で、支払処理が完了すると（支払が成立すると）、ステップS90において、商品発送のための処理が行われる。具体的には、ショッピングサーバ6-2は、例えば、ユーザAの住所を、配送先として、個人サーバ5から取得し、配送を管理する他のサーバ（図示せず）（以下、配送サーバと称する）に送信する。配送業者は、配送サーバから得られた配送先に、ユーザAにより購入された商品を配送する。

【0184】

ステップS91において、ショッピングサーバ6-2は、配送処理の内容を、パーソナルコンピュータ3-3に送信する。パーソナルコンピュータ3-3は、それを受信し、表示する。これにより、ユーザAは、配送手続きが完了したことを（例えば、配送先が決定したことを）、を確認することができる。

【0185】

なお、配送サーバは、個人サーバ5に、配送の状況（例えば、商品の出荷日、現在保管されている配送センター）を、例えば、定期的に提供するようになされ

ているので、ユーザAは、携帯端末2を介して、その情報を参照することができる。

【0186】

また、配送先が、個人サーバ5に個人情報として記憶されていない場合、ユーザAは、携帯端末2を操作して、希望する配信先を、ショッピングサーバ6-2に通知することができる。また、配信先を、例えば、ユーザAの住所で指定する他、「住所から最も近い、コンビニエンスストア」など、抽象的に指定することもできる。この場合、ショッピングサーバ6-2は、個人サーバ5から取得したユーザAの住所から最も近いコンビニエンスストアを探し出し、そこを配送先として、配送サーバに通知する。

【0187】

また、図16（図15）の例では、パーソナルコンピュータ3-3を介してネットショッピングを行ったが、このパーソナルコンピュータ3-3は、ユーザAが所有するものに限られない。例えば、このサービス提供システムの業者が、パーソナルコンピュータ3-3（ネットワークアクセスポート）を、例えば、レストラン、または街頭に配置すれば、ユーザAは、それを利用して、上述したようなサービスの提供を受けることができる。

【0188】

しかしながら、この場合、ネットワークアクセスポートを利用したユーザAに、このときの、サービス提供システムの使用料等を請求する必要がある。図17には、サービス提供システムの使用料を管理するネットワークアクセスポート管理サーバ（以下、管理サーバと略称する）71が図示されている。管理サーバ71は、ネットワーク4を介してネットワークアクセスポート3と個人サーバ5と通信して、URL4により特定される、使用料の精算処理を実行する。

【0189】

次に、サービス提供システムの使用料に対する精算処理の手順を、図18のフローチャートを参照して説明する。

【0190】

ステップS101において、ネットワークアクセスポート3は、一連のトラン

ザクションで転送したデータの量（例えば、携帯端末2または個人サーバ5に転送したデータ量）を算出する。

【0191】

次に、ステップS102において、ネットワークアクセスポート3は、個人サーバ5に、ステップS101で算出したデータ転送量、URL4、および自分自身の位置を示す情報（位置情報）を送信するとともに、URL4により特定される処理を実行する管理サーバ71との通信を要求する。個人サーバ5は、それらのデータを受信するとともに、その要求を認識する。なお、個人サーバ5は、受信した位置情報を、ユーザAの個人情報として記憶する。また、ネットワークアクセスポート3は、URL4を保持している。

【0192】

ステップS103において、個人サーバ5と管理サーバ71との通信が確立されると、ステップS104において、個人サーバ5は、ステップS102で受信した、位置情報、URL4、およびデータ転送量を、管理サーバ71に送信する。管理サーバ71は、それらを受信する。

【0193】

次に、ステップS105において、管理サーバ71は、ユーザ認証を、個人サーバ5に対して要求する。ステップS106において、個人サーバ5は、認証データによるユーザ認証を行う。ここでの処理は、図6のステップS7における処理と同様であるので、その説明は省略する。

【0194】

ステップS106で、ユーザAが、正規のユーザであると認証されると、ステップS107において、管理サーバ71は、ステップS104で受信した位置情報に基づいて、ネットワークアクセスポート3が不正利用されているか否かを判定する。

【0195】

例えば、ユーザAの契約において、利用地域が制限されている場合、その位置情報が、契約地域外の地域を示している場合、不正利用（契約外の利用）と判定される。また、アクセス間隔（時間）から見て、到底移動できない距離だけ離れ

ているネットワークアクセスポートのそれぞれを介して、アクセスがあった場合、不正利用されていると判定される。

【0196】

ステップS107で、不正利用されていないと判定された場合、ステップS108に進み、支払処理が行われる。具体的には、管理サーバ71は、URL4により特定される決済処理を実行する。これにより、ステップS101で算出されたデータ転送量に応じた、システムの使用料金の支払が行われる。

【0197】

ステップS107で、不正利用されていると判定された場合、ステップS109に進み、所定の処理が実行される。

【0198】

ステップS108またはステップS109の後、処理は終了する。なお、ここでは、管理サーバ71が、ネットワークアクセスポート3の位置情報に基づいて、ネットワークアクセスポート3の不正利用を判定する場合を例として説明したが、上述した、例えば、サービスサーバ6-1が、精算装置3-1の位置情報を取得し、精算装置3-1が不正利用されているか否かを判定することもできる。

【0199】

また、図1、14、15、17の例では、一人のユーザAによる利用について説明したが、実際は、図19に示すように、他のユーザ（ユーザB）も、他の携帯端末Bで、このシステムを利用する。すなわち、個人サーバ5は、多くのユーザの個人情報を、それぞれのURL1に基づいて管理している。

【0200】

ここで、個人サーバ5において、ユーザAの個人情報として管理されている、ユーザAが購入したコンテンツを、ユーザBが利用する場合の処理手順を説明する。

【0201】

携帯端末2または携帯端末Bから、ユーザAが購入した所定のコンテンツを、ユーザBが使用する旨が通知されると、個人サーバ5は、そのコンテンツを記憶している場所（アドレス）を、携帯端末Bに送信する。携帯端末Bは、それを受

信し、記憶する。ユーザBは、コンテンツを利用したいとき、携帯端末Bを操作して、先に記憶したアドレスに従って、コンテンツを取得する。

【0202】

このようにすることで、個人サーバ5は、コンテンツを重複して保持する必要がない（同一のコンテンツを、ユーザAおよびユーザBの個人情報として保持する必要がない）。また、ユーザBが実際にコンテンツを利用するまでは、携帯端末Bは、それを保持する必要がない。すなわち、個人サーバ5または携帯端末Bは、コンテンツを効率よく保持することができる。

【0203】

なお、購入されたコンテンツなどは、上述したように、ネットワーク4を介して転送され得るので、転送可能な情報として個人サーバ5に記憶されるが、ユーザの、住所、電話番号等の情報は、通常転送されないので、転送できない情報として個人サーバ5に記憶されるようになされている。

【0204】

図20は、本発明を適用したサービス提供システムの他の利用例を示している。この場合、サービス提供システムにより電車の改札処理が行われる。

【0205】

改札機3-4は、ユーザAが入札する駅Aの改札口に設置されている改札機であり、改札機3-5は、ユーザAが出札する駅Bの改札口に設置されている改札機である。改札機3-4、3-5は共に、ネットワークアクセスポートとしての機能を有し、駅サーバ6-3および駅サーバ6-4と通信する。

【0206】

駅サーバ6-3は、URL2-1により特定される、駅Aの改札機3-4での入札に関する情報を管理する処理を実行し、駅サーバ6-4は、URL2-2により特定される、駅Bの改札機3-5での出札に関する情報を管理する処理を実行する。

【0207】

次に、入札処理の手順を、図21のフローチャートを参照して説明する。

【0208】

ステップ S 1 1 1 において、駅 A の改札機 3 - 4 は、URL 2 - 1、入札時刻、および駅 A の ID を、携帯端末 2 に送信する。携帯端末 2 は、それらを受信する。このとき、ユーザ A（携帯端末 2）は、携帯端末 2 と改札機 3 - 4 との短距離通信が可能となる程度に、改札機 3 - 4 に近づいているものとする。

【 0 2 0 9 】

次に、ステップ S 1 1 2 において、携帯端末 2 は、個人サーバ 5 に、ステップ S 1 1 1 で受信した URL 2 - 1、入札時刻、および駅 A の ID を、改札機 3 - 4 およびネットワーク 4 を介して送信するとともに、URL 2 - 1 により特定される処理を実行する駅サーバ 6 - 3 との通信を要求する。個人サーバ 5 は、携帯端末 2 から送信されたデータを受信するとともに、その要求を認識する。個人サーバ 5 は、受信したデータを、ユーザ A の個人情報として記憶する。

【 0 2 1 0 】

ステップ S 1 1 2 の処理を具体的に説明すると、携帯端末 2 の CPU 2 1 は、ステップ S 1 1 1 で受信した情報を、表示部 2 4 に表示させる。ユーザ A は、表示部 2 4 に表示された情報を確認すると、入力部 2 3 に対して所定の操作を行う。これにより、携帯端末 2 は、ステップ S 1 1 1 で受信した情報を、個人サーバ 5 に送信する。

【 0 2 1 1 】

ステップ S 1 1 3 において、個人サーバ 5 と駅サーバ 6 - 3 との通信が確立されると、ステップ S 1 1 4 において、個人サーバ 5 は、ステップ S 1 1 2 で受信した入札時刻および駅 A の ID を、URL 1 とともに、駅サーバ 6 - 3 に送信する。駅サーバ 6 - 3 は、それらを受信する。

【 0 2 1 2 】

次に、ステップ S 1 1 5 において、駅サーバ 6 - 3 は、個人サーバ 5 に対して、ユーザ認証を要求する。個人サーバ 5 は、その要求を認識する。

【 0 2 1 3 】

ステップ S 1 1 6 において、認証データによるユーザ認証が行われる。ここでの処理は、図 6 のステップ S 7 における処理と同様であるので、その説明は省略する。

【 0 2 1 4 】

ステップ S 1 1 6 で、ユーザ A が正規のユーザであると認証されると、ステップ S 1 1 7 において、駅サーバ 6 - 3 は、ステップ S 1 1 4 で受信したデータを、記憶する。その後、処理は終了する。

【 0 2 1 5 】

次に、出札処理の手順を、図 2 2 のフローチャートを参照して説明する。

【 0 2 1 6 】

ステップ S 1 2 1 において、駅 B の改札機 3 - 5 は、URL 2 - 2、出札時刻、および駅 B の ID を、携帯端末 2 に送信する。携帯端末 2 は、それらを受信する。このとき、ユーザ A（携帯端末 2）は、携帯端末 2 と改札機 3 - 5 との短距離通信が可能となる程度に、改札機 3 - 5 に近づいているものとする。

【 0 2 1 7 】

次に、ステップ S 1 2 2 において、携帯端末 2 は、個人サーバ 5 に、ステップ S 1 2 1 で受信した URL 2 - 2、出札時刻、および駅 B の ID を、改札機 3 - 5 およびネットワーク 4 を介して送信するとともに、URL 2 - 2 により特定される処理を実行する駅サーバ 6 - 4 との通信を要求する。個人サーバ 5 は、携帯端末 2 から送信されたデータを受信するとともに、その要求を認識する。

【 0 2 1 8 】

ステップ S 1 2 2 の処理を具体的に説明すると、携帯端末 2 の CPU 2 1 は、ステップ S 1 2 1 で受信したデータを、表示部 2 4 に表示させる。ユーザ A は、表示部 2 4 に表示された情報を確認し、入力部 2 3 に対して所定の操作を行う。これにより、携帯端末 2 は、ステップ S 1 2 1 で受信した情報を、個人サーバ 5 に送信する。

【 0 2 1 9 】

ステップ S 1 2 3 において、個人サーバ 5 と駅サーバ 6 - 4 との通信が確立されると、ステップ S 1 2 4 で、個人サーバ 5 は、ステップ S 1 2 2 で受信した出札時刻および駅 B の ID を、URL 1 とともに、駅サーバ 6 - 4 に送信する。駅サーバ 6 - 4 は、それらを受信する。

【 0 2 2 0 】

ステップ S 1 2 5 において、駅サーバ 6 - 4 は、個人サーバ 5 に対して、ユーザ認証を要求する。個人サーバ 5 は、その要求を認識する。

【 0 2 2 1 】

次に、ステップ S 1 2 6 において、認証データによるユーザ認証が行われる。ここでの処理は、図 6 のステップ S 7 における処理と同様であるので、その説明は省略する。

【 0 2 2 2 】

ステップ S 1 2 6 で、ユーザ A が正規のユーザであると認証されると、ステップ S 1 2 7 において、料金算出処理が行われる。ここでの処理は、図 2 3 のフローチャートに示されている。

【 0 2 2 3 】

ステップ S 1 3 1 において、駅サーバ 6 - 4 は、個人サーバ 5 と通信し、ユーザ A の個人情報として記憶されている駅 A の ID (図 2 1 のステップ S 1 1 2) を取得する。

【 0 2 2 4 】

ステップ S 1 3 2 において、駅サーバ 6 - 4 は、ステップ S 1 3 1 で取得した駅 A の ID と、ステップ S 1 2 4 で受信した駅 B の ID に基づいて、料金を算出する。その後、処理は終了し、図 2 2 のステップ S 1 2 8 に進む。

【 0 2 2 5 】

ステップ S 1 2 8 において、支払処理が行われる。駅サーバ 6 - 4 は、ステップ S 1 2 7 で算出された料金の振り込み先を、個人サーバ 5 に通信する。個人サーバ 5 は、通知された振込先のサーバ (図示せず) に対して、所定の振り込み処理を行う。その後、処理は終了する。

【 0 2 2 6 】

図 2 4 は、本発明を適用したサービス提供システムの他の利用例を示している。この場合、サービス提供システムにより、遊園地のアトラクションを、1 日に限って自由に利用することができる入場券 (1 日フリーチケット) の券売処理および改札処理 (ゲート処理) が行われる。

【 0 2 2 7 】

券売機 3 - 6 は、遊園地の入場券を発券する装置である。ゲート機 3 - 7 は、所定のアトラクション付近に設定されているゲートであり、そのアトラクションを行う場合は、ユーザ A は、必ずゲート機 3 - 7 のゲート（図示せず）を通過しなければならない。

【 0 2 2 8 】

券売機 3 - 6 およびゲート機 3 - 7 は共に、ネットワークアクセスポートとしての機能を有し、チケットサーバ 6 - 5 およびゲートサーバ 6 - 6 とネットワーク 4 を介して通信する。

【 0 2 2 9 】

チケットサーバ 6 - 5 は、URL 2 - 1 により特定される、発券した入場券に関する情報を管理する処理を実行し、ゲートサーバ 6 - 6 は、URL 2 - 2 により特定される、ゲート機 3 - 7 のゲートの開閉を制御する処理を実行する。

【 0 2 3 0 】

次に、発券処理の手順を、図 2 5 のフローチャートを参照して説明する。

【 0 2 3 1 】

ステップ S 1 4 1 において、券売機 3 - 6 は、URL 2 - 1 と、利用可能が日付等の、1 日フリーチケットの利用に関する情報（以下、チケット情報）を、携帯端末 2 に送信する。携帯端末 2 は、それらを受信する。

【 0 2 3 2 】

なお、このとき、ユーザ A は、券売機 3 - 6 の操作パネル（図示せず）に対して、1 日フリーチケットを購入するための操作を行う。また、ユーザ A（携帯端末 2）は、携帯端末 2 と券売機 3 - 6 との短距離通信が可能となる程度に、券売機 3 - 6 に近づいているものとする。

【 0 2 3 3 】

ステップ S 1 4 2 において、携帯端末 2 は、個人サーバ 5 に、ステップ S 1 4 1 で受信した URL 2 - 1 およびチケット情報を送信するとともに、URL 2 - 1 により特定される処理を実行するチケットサーバ 6 - 5 との通信を要求する。個人サーバ 5 は、携帯端末 2 から送信されたデータを受信するとともに、その要求を認識する。

【0234】

ステップS142での処理を具体的に説明すると、携帯端末2のCPU21は、ステップS142で受信した情報を、表示部24に表示させる。ユーザAは、表示部24に表示された情報を確認すると、入力部23に対して所定の操作を行う。これにより、携帯端末2は、その操作に基づいて、ステップS141で受信した情報を、個人サーバ5に送信する。

【0235】

ステップS143において、個人サーバ5とチケットサーバ6-5との通信が確立すると、ステップS144において、個人サーバ5は、ステップS142で受信したチケット情報を、URL1とともに、チケットサーバ6-5に送信する。チケットサーバ6-5は、それを受信する。

【0236】

ステップS145において、チケットサーバ6-5は、個人サーバ5に対して、ユーザ認証を要求する。個人サーバ5は、その要求を認識する。

【0237】

次に、ステップS146において、認証データによるユーザ認証が行われる。ここでの処理は、図6のステップS7における処理と同様であるので、その説明は省略する。

【0238】

ステップS146で、ユーザAが正規のユーザであると認証されると、ステップS147において、発券処理が行われる。ここでの処理の詳細は、図26のフローチャートに示されている。

【0239】

ステップS151において、チケットサーバ6-5は、ステップS144で受信したチケット情報に基づいて、有効期限を決定するとともに、料金を算出する。この例の場合、有効期限は、本日の終了時刻とされる。

【0240】

次に、ステップS152において、チケットサーバ6-5は、ステップS151で決定した有効期限を、ステップS144で受信したURL1と対応させて記

憶する。

【0241】

ステップS153において、支払処理が行われる。チケットサーバ6-5は、ステップS151で算出した料金の振り込み先を、個人サーバ5に通信する。個人サーバ5は、通知された振り込み先のサーバ（図示せず）に対して、所定の振り込み処理を行う。

【0242】

ステップS153で、支払処理が完了すると、ステップS154において、チケットサーバ6-5は、ステップS151で決定した有効期限等からなるチケット情報を、個人サーバ5に送信する。個人サーバ5は、それを受信する。

【0243】

ステップS155において、個人サーバ5は、ステップS154で受信したチケット情報を、ユーザAの個人情報として記憶する。

【0244】

その後、処理は終了し、図25に戻り、発券処理が終了する。

【0245】

次に、ゲート処理の手順を、図27のフローチャートを参照して説明する。

【0246】

ステップS161において、ゲート機3-7は、URL2-2を、携帯端末2に送信する。携帯端末2は、それを受信する。なお、このとき、ユーザAは、携帯端末2とゲート機3-7との短距離通信が行われる程度にゲート機3-7に近づいているものとする。

【0247】

次に、ステップS162において、携帯端末2は、個人サーバ5に、ステップS161で受信したURL2-2を送信するとともに、URL2-2により特定される処理を実行するゲートサーバ6-6との通信を要求する。個人サーバ5は、携帯端末2から送信されたURL2-2を受信するとともに、その要求を認識する。

【0248】

ステップS163において、個人サーバ5とゲートサーバ6-6との通信が確立されると、ステップS164において、個人サーバ5は、図26のステップS155で記憶したチケット情報を、ゲートサーバ6-6に送信する。ゲートサーバ6-6は、それを受信する。

【0249】

ステップS165において、ゲートサーバ6-6は、チケットサーバ6-5にアクセスし、URL1とともに記憶されている有効期限を取得し、それがステップS164で受信したチケット情報に示される有効期限と一致し、かつ、その期限が切れていないか否か判定する。すなわち、ユーザAが、ゲート機3-7を通過できるか否かが判定される。

【0250】

ステップS165で、通過できると判定された場合、ステップS166に進み、ゲート機3-7のゲートが開放される。具体的には、ゲートサーバ6-6は、ゲートを開放させる指令を、ゲート機3-7に送信し、ゲート機3-7は、その指令に従い、ゲートを開放する。

【0251】

ステップS165で、通過できないと判定された場合、ステップS167に進み、ゲート機3-7のゲートは開放されず、所定のメッセージが出力される。

【0252】

ステップS166またはステップS167の後、ゲート処理は終了する。

【0253】

次に、ステップS147（発券処理）の他の処理について、図28のフローチャートを参照して説明する。

【0254】

ステップS171において、チケットサーバ6-5は、図25のステップS144で受信したチケット情報に基づいて、有効期限を決定するとともに、料金を算出する。

【0255】

次に、ステップS172において、チケットサーバ6-5は、ステップS17

1で決定した有効期限を、URL 1と対応させて記憶するとともに、ゲートサーバ6-6に送信する。ゲートサーバ6-6は、それを受信し、記憶する。

【0256】

ステップS173において、支払処理が行われる。

【0257】

次に、ステップS174において、個人サーバ5は、ユーザAの顔写真データを、チケットサーバ6-5に送信する。チケットサーバ6-5は、それを受信する。

【0258】

ステップS175において、チケットサーバ6-5は、ステップS174で受信した顔写真データをURL 1と対応させて記憶するとともに、顔写真データを、ゲートサーバ6-6に送信する。ゲートサーバ6-6は、それを受信し、URL 1と対応させて記憶する。

【0259】

その後、処理は終了する。

【0260】

次に、この発券処理に対応するゲート処理を、図29のフローチャートを参照して説明する。

【0261】

ステップS181において、携帯端末2は、URL 1を、ゲート機3-7を介してゲートサーバ6-6に送信する。ゲートサーバ6-6は、それを受信する。なお、ユーザAは（携帯端末2）は、携帯端末2とゲート機3-7との短距離通信が可能となる程度にゲート機3-7に近づいているものとする。

【0262】

ステップS182において、ゲートサーバ6-6は、図28のステップS172で記憶した有効期限を読み出し、ステップS183において、その有効期限が切れているか否かを判定する。すなわち、ユーザAが、ゲート機3-7のゲートを通過することができるか否かが判定される。

【0263】

ステップ S 1 8 3 で、通過できると判定された場合、ステップ S 1 8 4 において、ゲートサーバ 6 - 6 は、ステップ S 1 7 5 で記憶した顔写真データとともに、ゲートを開放する指令を、ゲート機 3 - 7 に送信する。

【 0 2 6 4 】

ステップ S 1 8 5 において、ゲート機 3 - 7 は、ステップ S 1 8 4 で受信した顔写真データに対応する画像を表示するとともに、ゲートを開放する。

【 0 2 6 5 】

ステップ S 1 8 3 で、通過できないと判定された場合、ステップ S 1 8 6 に進み、処理の処理が実行される。

【 0 2 6 6 】

ステップ S 1 8 5 またはステップ S 1 8 6 の後、処理は終了する。

【 0 2 6 7 】

なお、図 2 5 の例では、認証データによるユーザ認証により、ユーザ A が正規のユーザであると認証された場合、チケットが発券される場合を例として説明したが、そのユーザ認証処理を省略することもできる。

【 0 2 6 8 】

しなしながら、この場合、チケットサーバ 6 - 5 に記憶された URL 1 (図 2 6 のステップ S 1 5 2) をユーザ A 以外の第 3 者が取得すれば、その URL 1 をゲート機 3 - 7 に送信することで (図 2 7 のステップ S 1 6 1)、不正にゲート機 3 - 7 を通過することができる (不正にアトラクションを利用することができる)。

【 0 2 6 9 】

図 3 0 には、認証データによるユーザ認証が省略された場合でも不正利用を防止することができるシステムの構成例が示されている。

【 0 2 7 0 】

通過監視装置 3 - 8 は、開放自在なゲート 3 - 8 A を有しており、ユーザが、図中矢印方向に移動する通路 A の所定の地点 A に設置されている。ユーザは、その通路を通る際、必ず通過監視装置 3 - 8 のゲート 3 - 8 A を通過しなければならない。

【0271】

通過監視装置3-8はまた、携帯端末2に対するネットワークアクセスポートとしての機能を有しており、携帯端末2と通信するとともに、ネットワーク4を介してチケットサーバ6-5および監視サーバ6-7と通信する。

【0272】

通過監視装置3-9は、通過監視装置3-8と同様に、開放自在なゲート3-9Aを有しており、地点Aから、図中矢印で示される進行方向に対して、所定の距離だけ離れた地点Bに設置されている。地点Aと地点B間は、その間を移動するのに（歩くのに）、所定の時間以上かかる分だけ離れている。

【0273】

通過監視装置3-9も、携帯端末2に対するネットワークアクセスポートとしての機能を有しており、携帯端末2と通信し、ネットワーク4を介してチケットサーバ6-5および監視サーバ6-7と通信する。

【0274】

監視サーバ6-7は、URL2-3により特定される、通過監視装置3-9のゲート3-9Aを通過しようとしているユーザが、チケットを不正利用しているか否かを監視する処理を実行する。

【0275】

次に、通過監視装置3-8の動作を、図31のフローチャートを参照して説明する。

【0276】

ステップS191において、通過監視装置3-8は、URL2-3、検知時刻、および自分自身のIDを、携帯端末2に送信する。携帯端末2は、それを受信する。このとき、ユーザA（携帯端末2）は、携帯端末2と通過監視装置3-8との短距離通信が可能となる程度に、通過監視装置3-8に近づいている。

【0277】

次に、ステップS192において、携帯端末2は、個人サーバ5に、ステップS191で受信したURL2-3、検知時刻、およびIDを、通過監視装置3-8を介して送信するとともに、URL2-3により特定される処理を実行する監

視サーバ6-7との通信を要求する。個人サーバ5は、携帯端末2から送信されたデータを受信するとともに、その要求を認識する。

【0278】

ステップS193において、個人サーバ5と監視サーバ6-7との通信が確立されると、ステップS194において、個人サーバ5は、ステップS192で受信した検知時刻およびIDを、URL1とともに、監視サーバ6-7に送信する。監視サーバ6-7は、それらを受信する。

【0279】

次に、ステップS195において、監視サーバ6-7は、ステップS194で受信した検知時刻、ID、およびURL1をそれぞれ対応させて記憶する。

【0280】

ステップS196において、監視サーバ6-7は、チケットサーバ6-5と通信し、ステップS194で記憶したURL1が、チケットサーバ6-5に管理されているか否かを判定する（図26のステップS152の処理で、URL1が記憶されているか否かを判定する）。すなわち、ユーザAが、正規にチケットを購入し、ゲート3-8Aを通過することができる者であるか否かが判定される。

【0281】

ステップS196で、通過することができる者であると判定された場合、ステップS197に進む。

【0282】

ステップS197において、監視サーバ6-7は、通過監視装置3-8のゲート3-8Aを開放させる処理を行う。これにより、そのゲート3-8Aが開放し、ユーザAは、そこを通過することができる。

【0283】

ステップS196で、通過することができない者であると判定された場合、ステップS198に進み、監視サーバ6-7は、所定の警告処理を実行する。

【0284】

ステップS197またはステップS198での処理が行われた後、通過監視処理は終了する。

【0285】

次に、通過監視装置3-9の動作を、図32のフローチャートを参照して説明する。

【0286】

ステップS201において、通過監視装置3-9は、URL2-3、検知時刻、および自分自身のIDを、携帯端末2に送信する。携帯端末2は、それらを受信する。このとき、ユーザA（携帯端末2）は、携帯端末2と通過監視装置3-9との短距離通信が可能となる程度に、通過監視装置3-9に近づいている。

【0287】

次に、ステップS202において、携帯端末2は、個人サーバ5に、ステップS201で受信したURL2-3、検知時刻、およびIDを、通過監視装置3-9を介して送信するとともに、URL2-3により特定される処理を実行する監視サーバ6-7との通信を要求する。個人サーバ5は、携帯端末2から送信されたデータを受信するとともに、その要求を認識する。

【0288】

ステップS203において、個人サーバ5と監視サーバ6-7との通信が確立されると、ステップS204において、個人サーバ5は、ステップS202で受信した検知時刻およびIDを、URL1とともに、監視サーバ6-7に送信する。監視サーバ6-7は、それを受信する。

【0289】

次に、ステップS205において、監視サーバ6-7は、図31のステップS195でURL1と対応して記憶した、通過監視装置3-8での検知時刻を読み出し、ステップS206において、ステップS204で受信した検知時刻との差（時間）を算出し、その時間が、予め決められた時間（地点Aから地点Bに移動するのに必要な時間）Tより短いかな否かを判定する。

【0290】

通過監視装置3-8と通過監視装置3-9は、移動するのに時間Tかかるだけ離れているので、ユーザAが、通過監視装置3-8（ゲート3-8A）を通過した後、時間T以内に、通過監視装置3-9により検知される場合はない。すなわ

ち、時間T以内に、URL1が通過監視装置3-9に送信された場合、URL1が、第3者により不正に保持されているものとすることができる。従って、ここでの処理では、URL1が不正利用されているか否かが判定され、ユーザAがゲート3-9Aを通過することができる者であるか否かが判定される。

【0291】

ステップS206で、通過することができる者であると判定された場合、ステップS207に進み、監視サーバ6-7は、通過監視装置3-9のゲート3-9Aを開放させる処理を行う。これにより、ゲート3-9Aが開放し、ユーザAは、そこを通過することができる。

【0292】

ステップS206で、通過することができない者であると判定された場合、ステップS208に進み、監視サーバ6-7は、所定の警告処理を実行する。

【0293】

ステップS207またはステップS208での処理が行われた後、この通過監視処理は終了する。

【0294】

図33は、本発明を適用したサービス提供システムの他の利用例を示している。この場合は、サービス提供システムにより、有料道路の通行料金の支払処理が行われる。ユーザAは、携帯端末2を携帯して自動車Aに搭乗している。

【0295】

入門ゲート機3-10は、携帯端末2に対するネットワークアクセスポートとしての機能を有する装置で、有料道路の入口に設置されている。

【0296】

料金ゲート機3-11は、携帯端末2に対するネットワークアクセスポートとしての機能を有する装置で、有料道路の出口に設置されている。料金ゲート機3-11はまた、ビデオカメラ（図示せず）を有し、通過する自動車の車両番号を撮像するとともに、その結果得られた画像データから、車両番号を検出する。

【0297】

通行料金サーバ6-8は、個人サーバ5、入門ゲート機3-10、または料金

サーバ 3-11 と、ネットワーク 4 を介して通信し、URL 2 により特定される、有料道路の通行料金の支払に関する処理を実行する。通行料金サーバ 6-8 は、自動車（自動車 A）の車両番号を、所定の有効期限とともに予め記憶している。

【0298】

個人サーバ 5 は、ユーザ A の自動車の車両番号を、ユーザ A の個人情報として記憶している。

【0299】

次に、この支払処理の手順を、図 34 のフローチャートを参照して説明する。

【0300】

ステップ S221 において、携帯端末 2 は、URL 1 を、入門ゲート機 3-10 に送信する。入門ゲート機 3-10 は、それを受信する。

【0301】

具体的には、自動車 A（携帯端末 2）が、携帯端末 2 と入門ゲート機 3-10 との短距離通信が可能となる程度にまで、入門ゲート機 3-10 に近づいたとき、ユーザ A は、携帯端末 2 の入力部 23 に対して所定の操作を行う。これにより、携帯端末 2 は、上記したデータを、入門ゲート機 3-10 に送信する。

【0302】

次に、ステップ S222 において、入門ゲート機 3-10 は、ステップ S221 で受信した URL 1 とその受信時刻を、通行料金サーバ 6-8 に送信する。通行料金サーバ 6-8 は、それらを受信する。

【0303】

ステップ S223 において、通行料金サーバ 6-8 は、ステップ S222 で受信した URL 1 と受信時刻を記憶する。

【0304】

次に、ステップ S224 において、携帯端末 2 は、URL 1 を、料金ゲート機 3-11 に送信する。料金ゲート機 3-11 は、それを受信する。

【0305】

自動車 A は、有路道路を走行し、料金ゲート機 3-11 が設置されている出口

から降り、料金ゲート機 3-11 に近づいたとき（携帯端末 2 と料金ゲート機 3-11 との短距離通信が可能となる程度にまで近づいたとき）、ユーザ A は、携帯端末 2 の入力部 23 に対して所定の操作を行う。これにより、携帯端末 2 は、URL 1 を、料金ゲート機 3-11 に送信する。

【0306】

ステップ S 2 2 5 において、料金ゲート機 3-11 は、通過する自動車 A を撮像し、その結果得られた画像データから車両番号を検出する。料金ゲート機 3-11 は、検出した車両番号を、ステップ S 2 2 4 で受信した URL 1 とその受信時刻とともに、通行料金サーバ 6-8 に送信する。通行料金サーバ 6-8 は、それらを受信する。

【0307】

ステップ S 2 2 6 において、通行料金サーバ 6-8 は、自動車 A が料金ゲート機 3-11 を通過することができるか否かを判定する。

【0308】

この例の場合、個人サーバ 5 と通行料金サーバ 6-8 の間において、ユーザ A に対する、認証データによるユーザ認証（例えば、図 6 のステップ S 7）が予め行われており、通行料金サーバ 6-8 は、ユーザ A が正規のユーザである情報を、その情報の有効期限、および車両番号とともに、URL 1 に対応させて記憶している。すなわち、ここでの処理（ステップ S 2 2 6）で、通行料金サーバ 6-8 は、ステップ S 2 2 5 で受信した車両番号と、URL 1 と対応させて予め記憶している車両番号とを照合し、同一であるか否かを判定し、またステップ S 2 2 3 で記憶した受信時刻が、URL 1 と対応させて予め記憶している有効期限内の時刻を示しているか否かを判定する。従って、車両番号が同一であり、かつ、有効期限内であると判定されたとき、自動車 A は、料金ゲート機 3-11 を通過することができるものと判定され、ステップ S 2 2 7 に進み、支払処理が行われる。

【0309】

一方、ステップ S 2 2 6 で、車両番号が同一ではなく、または有効期限内ではないと判定された場合、自動車 A は、料金ゲート機 3-11 を通過することがで

きないものと判定され、ステップ S 2 2 8 に進み、所定の警告処理が行われる。

【0 3 1 0】

図 3 5 は、本発明を適用したサービス提供システムの他の利用例を示している。この場合は、サービス提供システムにより、公共料金の精算処理が行われる。

【0 3 1 1】

精算装置 3 - 1 2 は、公共料金に関する契約または精算をする場合に操作される端末で、例えば、コンビニエンスストア等に設置されている。精算装置 3 - 1 2 はまた、携帯端末 2 に対するネットワークアクセスポートとしての機能を有している。

【0 3 1 2】

公共料金サーバ 6 - 9 は、ネットワーク 4 を介して、精算装置 3 - 1 2 および個人サーバ 5 と通信し、URL 2 により特定される公共料金に関する処理を実行する。

【0 3 1 3】

次に、このシステムを利用して公共料金の精算を行うための契約処理の手順を、図 3 6 のフローチャートを参照して説明する。

【0 3 1 4】

ステップ S 2 4 1 において、精算装置 3 - 1 2 は、URL 2 と契約情報を、携帯端末 2 に送信する。携帯端末 2 は、それを受信する。

【0 3 1 5】

このとき、ユーザ A は、精算装置 3 - 1 2 に対して、例えば、自分の名前など、契約情報を入力する操作を行う。これにより、精算装置 3 - 1 2 は、上述した情報を、携帯端末 2 に送信する。

【0 3 1 6】

次に、ステップ S 2 4 2 において、携帯端末 2 は、個人サーバ 5 に、ステップ S 2 4 1 で受信した URL 2 と契約情報を、精算装置 3 - 1 2 およびネットワーク 4 を介して送信するとともに、公共料金サーバ 6 - 9 との通信を要求する。

【0 3 1 7】

ステップ S 2 4 3 において、個人サーバ 5 と公共料金サーバ 6 - 9 との通信が

確立される。

【0318】

次に、ステップS244において、個人サーバ5は、ステップS242で受信した契約情報を、公共料金サーバ6-9に送信する。公共料金サーバ6-9は、それを受信する。

【0319】

ステップS245において、公共料金サーバ6-9は、ユーザ認証を、個人サーバ5に要求する。個人サーバ5は、その要求を認識する。

【0320】

ステップS246において、ユーザ認証が行われる。ここでの処理は、図6のステップS7における処理と同様であるので、その説明は省略する。

【0321】

次に、ステップS247において、契約処理が行われる。この処理の詳細は、図37にフローチャートに示されている。

【0322】

ステップS251において、公共料金サーバ6-9は、ステップS244で受信した契約情報に基づいて、契約期限を決定する。

【0323】

ステップS252において、公共料金サーバ6-9は、ステップS251で決定した契約期限をURL1に対応させて記憶するとともに、契約期限とURL2を、個人サーバ5に送信する。個人サーバ5は、それを受信する。

【0324】

ステップS253において、個人サーバ5は、ステップS252で受信したURL2と契約期限を記憶する。その後処理は、終了する。

【0325】

次に、公共料金の精算処理を、図38のフローチャートを参照して説明する。

【0326】

ステップS261において、個人サーバ5と公共料金サーバ6-9との通信が確立される。具体的には、公共料金サーバ6-9は、予め決められたタイミング

(例えば、毎月所定の日)に、個人サーバ5に対して、接続を要求する。個人サーバ5は、それに応答する。

【0327】

ステップS262において、公共料金サーバ6-9は、公共料金の支払を、個人サーバ5に要求する。

【0328】

次に、ステップS263において、個人サーバ5は、URL2と対応して記憶した契約期限を参照し、それが切れているか否かを判定し、切れていないと判定した場合、ステップS264に進む。

【0329】

ステップS264において、支払処理が行われる。具体的には、個人サーバ5は、料金の振り込みサーバに対して振り込み処理を行う。個人サーバ5は、振り込み結果を、公共料金サーバ6-9に送信する。公共料金サーバ6-9は、それを記録する。

【0330】

ステップS263で、契約期限が切れていると判定された場合、ステップS265に進み、所定の処理が実行される。

【0331】

ステップS264またはステップS265の後、公共料金の支払処理は終了する。

【0332】

図39は、本発明を適用したサービス提供システムの他の利用例を示している。この場合、サービス提供システムを利用により、病院におけるカルテ(診療簿)が管理される。

【0333】

カルテ管理端末3-13は、カルテの内容を参照したいときに操作される端末で、例えば、病院内に設置されている。カルテ管理端末3-13はまた、携帯端末2に対するネットワークアクセスポートとしての機能を有している。

【0334】

カルテ管理サーバ 6-10 は、ネットワーク 4 を介して、カルテ管理端末 3-13 および個人サーバ 5 と通信し、URL 2 により特定される、カルテ情報を管理する処理を実行する。

【0335】

次に、このシステムを利用したカルテ情報を参照するための処理手順を、図 40 のフローチャートを参照して説明する。

【0336】

ステップ S 2 7 1 において、カルテ管理端末 3-13 は、URL 2 を、携帯端末 2 に送信する。携帯端末 2 は、それを受信する。

【0337】

ステップ S 2 7 2 において、携帯端末 2 は、個人サーバ 5 は、ステップ S 2 7 1 で受信した URL 2 を、カルテ管理端末 3-13 およびネットワーク 4 を介して送信するとともに、カルテ管理サーバ 6-10 との通信を要求する。

【0338】

ステップ S 2 7 3 において、個人サーバ 5 とカルテ管理サーバ 6-10 との通信が確立される。

【0339】

次に、ステップ S 2 7 4 において、カルテ管理サーバ 6-10 は、個人サーバ 5 に対して、ユーザ認証を要求する。個人サーバ 5 は、その要求を認識する。

【0340】

ステップ S 2 7 5 において、認証データによるユーザ認証が行われる。ここでの処理は、図 6 のステップ S 7 における場合と同様であるので、その説明は省略する。

【0341】

ステップ S 2 7 5 で、ユーザ A が正規のユーザであると認証されると、ステップ S 2 7 6 において、カルテ管理サーバ 6-10 は、ユーザ認証されたユーザ A のカルテ情報を、URL 1 の公開鍵で暗号化し、個人サーバ 5 に送信する。個人サーバ 5 は、それを受信する。なお、URL 1 の公開鍵は、ステップ S 2 7 5 における処理で、個人サーバ 5 からカルテ管理サーバ 6-10 に供給される。

【0342】

次に、ステップS277において、個人サーバ5は、ステップS276で受信したカルテ情報（URL1の公開鍵で暗号化されている）を、URL1の秘密鍵で解凍した後、携帯端末2の公開鍵で暗号化する。

【0343】

ステップS278において、個人サーバ5は、ステップS277で暗号化したカルテ情報を、カルテ管理端末3-13を介して、携帯端末2に送信する。携帯端末2は、それを受信する。

【0344】

次に、ステップS279において、携帯端末2は、ステップS278で受信したカルテ情報（携帯端末2の公開鍵で暗号化されている）を、携帯端末2の秘密鍵で解凍し、それを表示部24に表示する。これにより、ユーザAは、自分のカルテの内容を知ることができる。

【0345】

その後、処理は終了する。

【0346】

図41は、本発明を適用したサービス提供システムの他の利用例を示している。この例では、個人サーバ5、計算サーバ6-11、表示装置6-12、キーボード6-13、およびマウス6-14は、それぞれネットワークアクセスポート3およびネットワーク4を介して互いに接続し、いわゆるコンピュータを構成する。

【0347】

携帯端末2は、表示装置6-12、キーボード6-13、およびマウス6-14と、例えば、赤外線通信等を行い、それぞれが管理するURL2-2、URL2-3、およびURL2-4を取得する。携帯端末2は、取得したURL2-2、URL2-3、およびURL2-4の他、コンピュータにおけるCPU的役割を果たす計算サーバ6-11が管理するURL2-1を、個人サーバ5に送信するとともに、これらのURLに基づく情報の伝達の制御を、個人サーバ5に要求する。これにより、ユーザAによる、キーボード6-13およびマウス6-14

に対する操作に対応して、各種情報が、計算サーバ 6-11 乃至マウス 6-14 の間で送受信されるので、ユーザは、あたかも 1 台のコンピュータを利用している場合と同様に、例えば、計算処理等を行うことができる。

【0348】

なお、表示装置 6-12、キーボード 6-13、またはマウス 6-14 が、ユーザ A がよく使用するものである場合、それらが管理する URL 2 を、個人サーバ 5 が、ユーザ A の個人情報として記憶しておけば、新たにそれらの URL を取得する必要がなくなる。

【0349】

また、ユーザ A が、表示装置 6-12 の前にいる場合のみ利用できるようにすることができる。この場合、携帯端末 2 は、URL 1 を、表示装置 6-12 に転送し、表示装置 6-12 は、受信した URL 1 からの制御による場合のみ表示データ等を受信することができるようにする。

【0350】

このように、図 4 1 に示したような利用例によれば、コンピュータの本体がなくても、表示装置や入力装置さえあれば、コンピュータとしての機能を利用することができる。

【0351】

ところで、コンピュータ上において実行される文書作成プログラムは、頻度良く入力される言葉または文書が記憶され、キー入力により、その言葉または文書の途中までの文字が入力されると、その言葉または文書の全体が出力される機能を有する。従って、この機能により、ユーザは、その言葉または文書の全ての文字をキー入力する必要がないので、文書作成等を容易に行うことができる。

【0352】

そこで、例えば、図 4 1 の例の場合、そのような情報を、個人サーバ 5 が保持するようにし、必要に応じて、携帯端末 2 がそれを取得し、記憶することで、言葉や文書の全ての文字をキー入力しなくても、言葉や文書の全体を出力させることができる。

【0353】

なお、以上においては、携帯端末2に対するネットワークアクセスポート3は、所定の場所に固定されている場合を例として接続したが、図42に示すように、ユーザAが携帯する携帯電話（またはPHS）3-14を、ネットワークアクセスポートとして利用することができる。この場合、携帯端末2と、例えば、個人サーバ5との通信は、携帯電話3-14、基地局81、公衆電話網82、プロバイダ83、およびネットワーク4を介して行われる。

【0354】

また、図42の例では、携帯電話3-14は、携帯端末2に対するネットワークアクセスポートとして利用されるが、図43に示すように、携帯端末2としても利用することができる。なお、この場合、携帯電話3-14は、腕時計1の認証データ用ICチップと通信することができる機能を有している。

【0355】

上述した一連の処理は、ハードウェアにより実現させることもできるが、ソフトウェアにより実現させることもできる。一連の処理をソフトウェアにより実現する場合には、そのソフトウェアを構成するプログラムがコンピュータにインストールされ、そのプログラムがコンピュータで実行されることより、上述した、携帯端末2、個人サーバ5、またはサービスサーバ6-1等が機能的に実現される。

【0356】

図44は、上述のような携帯端末2、個人サーバ5、またはサービスサーバ6-1等として機能するコンピュータ501の一実施の形態の構成を示すブロック図である。CPU511にはバス515を介して入出力インタフェース516が接続されており、CPU511は、入出力インタフェース516を介して、ユーザから、キーボード、マウスなどよりなる入力部518から指令が入力されると、例えば、ROM512、ハードディスク514、またはドライブ520に装着される磁気ディスク531、光ディスク532、光磁気ディスク533、若しくは半導体メモリ534などの記録媒体に格納されているプログラムを、RAM513にロードして実行する。これにより、上述した各種の処理が行われる。さらに、CPU511は、その処理結果を、例えば、入出力インタフェース516を介して、LC

Dなどよりなる表示部517に必要な応じて出力する。なお、プログラムは、ハードディスク514やROM512に予め記憶しておき、コンピュータ501と一体的にユーザに提供したり、磁気ディスク531、光ディスク532、光磁気ディスク533、半導体メモリ534等のパッケージメディアとして提供したり、衛星、ネットワーク等から通信部519を介してハードディスク514に提供することができる。

【0357】

なお、本明細書において、記録媒体により提供されるプログラムを記述するステップは、記載された順序に沿って時系列的に行われる処理はもちろん、必ずしも時系列的に処理されなくとも、並列的あるいは個別に実行される処理をも含むものである。

【0358】

また、本明細書において、システムとは、複数の装置により構成される装置全体を表すものである。

【0359】

【発明の効果】

本発明の情報処理装置および方法、並びに記録媒体によれば、第1のネットワーク特定情報を記憶し、第2のネットワーク特定情報を取得し、ユーザを認証するために必要な認証データを取得し、取得された第2のネットワーク特定情報により特定される処理がサービスサーバにより実行されることで、サービスの提供を受けることができるように、第1のネットワーク特定情報により特定される個人情報管理する個人サーバに、第1のネットワーク特定情報および第2のネットワーク特定情報を含む制御情報を送信するようにしたので、例えば、情報処理装置を紛失しても、個人情報が第3者に渡ることを防止することができる。

【0360】

本発明の第1のサービス提供システムによれば、携帯端末が、第1のネットワーク特定情報を記憶し、第2のネットワーク特定情報を取得し、ユーザを認証するために必要な認証データを取得し、取得された第2のネットワーク特定情報により特定される処理が第2のサーバにより実行されることで、所定のサービスの

提供を受けることができるように、記憶されている第1のネットワーク特定情報により特定される個人情報管理する第1のサーバに、第1のネットワーク特定情報および第2のネットワーク特定情報を含む制御情報を供給し、取得された認証データを、第1のサーバに供給し、第1のサーバが、第1のネットワーク特定情報により特定される個人情報管理し、供給された制御情報に含まれる第2のネットワーク特定情報により特定される処理を実行する第2のサーバに、制御情報および個人情報に基づくサービスの提供を要求し、第2のサーバからの要求に基づいて、供給された認証データに基づきユーザを認証し、認証結果を、第2のサーバに供給し、第2のサーバが、第2のネットワーク特定情報により特定される処理を管理し、要求があったとき、ユーザの認証を第1のサーバに要求し、供給された認証結果が、ユーザが、第1のサービス提供システムの正規のユーザである旨を示しているとき、第2のネットワーク特定情報により特定される処理を、制御情報および個人情報に基づいて実行するようにしたので、例えば、情報処理装置を紛失しても、個人情報第3者に渡ることを防止することができる。

【0361】

本発明の第2のサービス提供システムによれば、携帯端末が、第1のネットワーク特定情報を記憶し、第2のネットワーク特定情報およびアクセスパターン検出のためのアクセス情報を、サービス端末から取得し、取得された第2のネットワーク特定情報により特定される処理が第2のサーバにより実行されることで、所定のサービスの提供を受けることができるように、記憶されている第1のネットワーク特定情報により特定される個人情報管理する第1のサーバに、第1のネットワーク特定情報、第2のネットワーク特定情報、およびアクセス情報を含む制御情報を、サービス端末に供給し、サービス端末が、第2のネットワーク特定情報を保持し、自分自身に対するアクセスから、アクセス情報を取得し、取得されるように、第2のネットワーク特定情報およびアクセス情報を、携帯端末に供給し、供給された制御情報を、第1のサーバに供給し、第1のサーバが、第1のネットワーク特定情報により特定される個人情報管理し、供給された制御情報に含まれる第2のネットワーク特定情報により特定される処理を実行する第2のサーバに、制御情報、個人情報、およびアクセス情報に基づくサービスの提供

を要求し、第2のサーバが、第2のネットワーク特定情報により特定される処理を管理し、要求に基づいて、第2のネットワーク特定情報により特定される処理を、制御情報、個人情報、およびアクセス情報に基づいて実行するようにしたので、例えば、情報処理装置を紛失しても、個人情報が第3者に渡ることを防止することができる。

【図面の簡単な説明】

【図1】

本発明を適用したサービス提供システムの利用例を示す図である。

【図2】

図1の腕時計1に組み込まれた認証データ用ICチップの構成例を示すブロック図である。

【図3】

図1の携帯端末2の構成例を示すブロック図である。

【図4】

図1の精算装置3-1の構成例を示すブロック図である。

【図5】

図1の個人サーバ5の構成例を示すブロック図である。

【図6】

精算処理を説明するフローチャートである。

【図7】

図6のステップS6の処理を説明するフローチャートである。

【図8】

図6のステップS7の処理を説明するフローチャートである。

【図9】

携帯端末2の他の構成例を示すブロック図である。

【図10】

商品券を利用した精算処理を説明するフローチャートである。

【図11】

図10のステップS47の処理を説明するフローチャートである。

【図 1 2】

携帯端末 2 の他の構成例を示すブロック図である。

【図 1 3】

精算処理を説明する他のフローチャートである。

【図 1 4】

本発明を適用したサービス提供システムの他の利用例を示す図である。

【図 1 5】

本発明を適用したサービス提供システムの他の利用例を示す図である。

【図 1 6】

ネットショッピング処理を説明するフローチャートである。

【図 1 7】

本発明を適用したサービス提供システムの他の利用例を示す図である。

【図 1 8】

システム使用料の精算処理を説明するフローチャートである。

【図 1 9】

本発明を適用したサービス提供システムの他の利用例を示す図である。

【図 2 0】

本発明を適用したサービス提供システムの他の利用例を示す図である。

【図 2 1】

入札処理を説明するフローチャートである。

【図 2 2】

出札処理を説明するフローチャートである。

【図 2 3】

図 2 2 のステップ S 1 2 7 の処理を説明するフローチャートである。

【図 2 4】

本発明を適用したサービス提供システムの他の利用例を示す図である。

【図 2 5】

発券処理を説明するフローチャートである。

【図 2 6】

図25のステップS147の処理を説明するフローチャートである。

【図27】

ゲート処理を説明するフローチャートである。

【図28】

図25のステップS147の他の処理を説明するフローチャートである。

【図29】

他のゲート処理を説明するフローチャートである。

【図30】

本発明を適用したサービス提供システムの他の利用例を示す図である。

【図31】

通過監視処理を説明するフローチャートである。

【図32】

他の通過監視処理を説明するフローチャートである。

【図33】

本発明を適用したサービス提供システムの他の利用例を示す図である。

【図34】

有料道路の料金自動支払処理を説明するフローチャートである。

【図35】

本発明を適用したサービス提供システムの他の利用例を示す図である。

【図36】

契約処理を説明するフローチャートである。

【図37】

図36のステップS247の処理を説明するフローチャートである。

【図38】

他の精算処理を説明するフローチャートである。

【図39】

本発明を適用したサービス提供システムの他の利用例を示す図である。

【図40】

カルテ管理処理を説明するフローチャートである。

【図 4 1】

本発明を適用したサービス提供システムの他の利用例を示す図である。

【図 4 2】

本発明を適用したサービス提供システムの他の利用例を示す図である。

【図 4 3】

本発明を適用したサービス提供システムの他の利用例を示す図である。

【図 4 4】

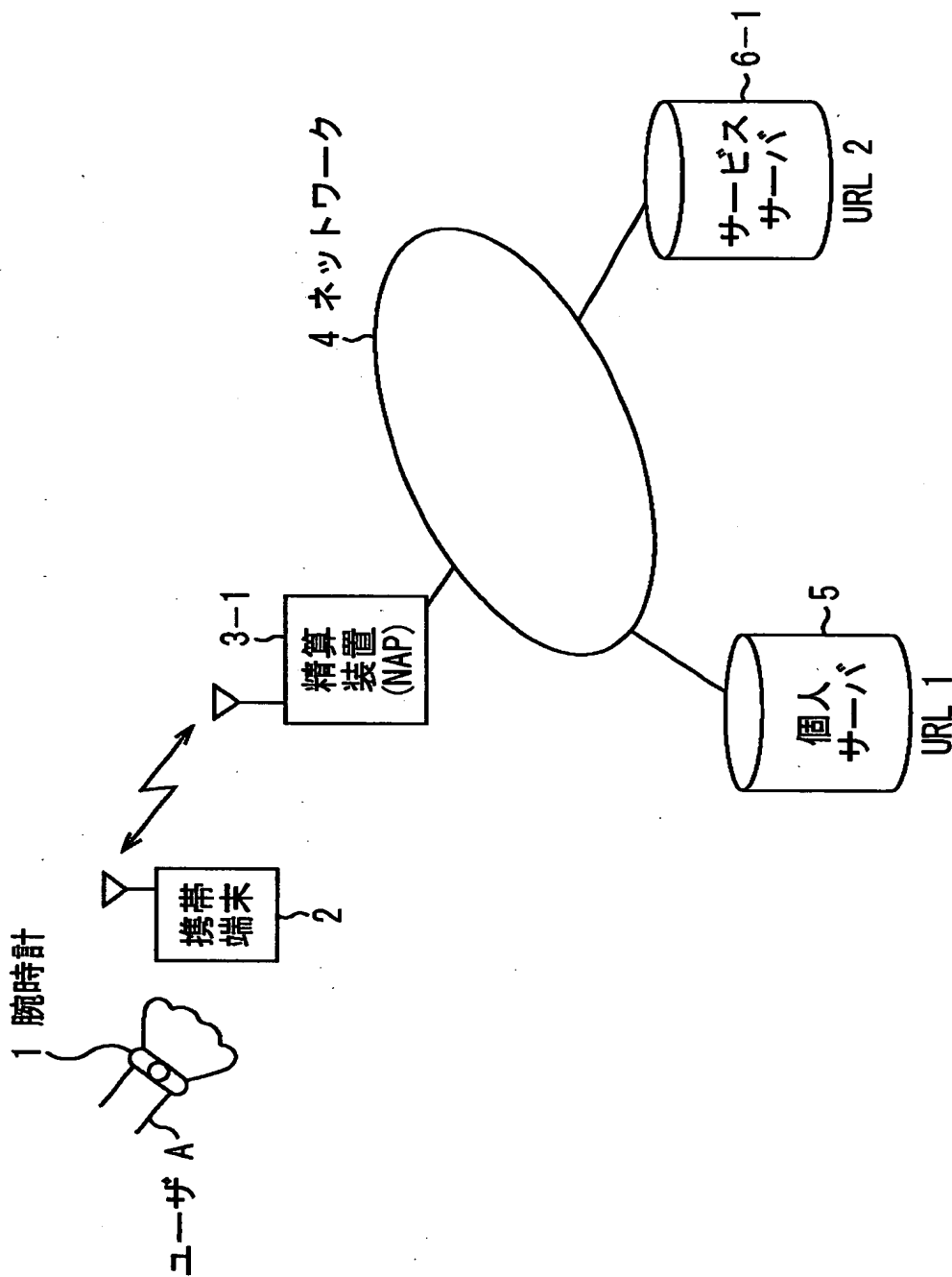
コンピュータ 501 の構成例を示すブロック図である。

【符号の説明】

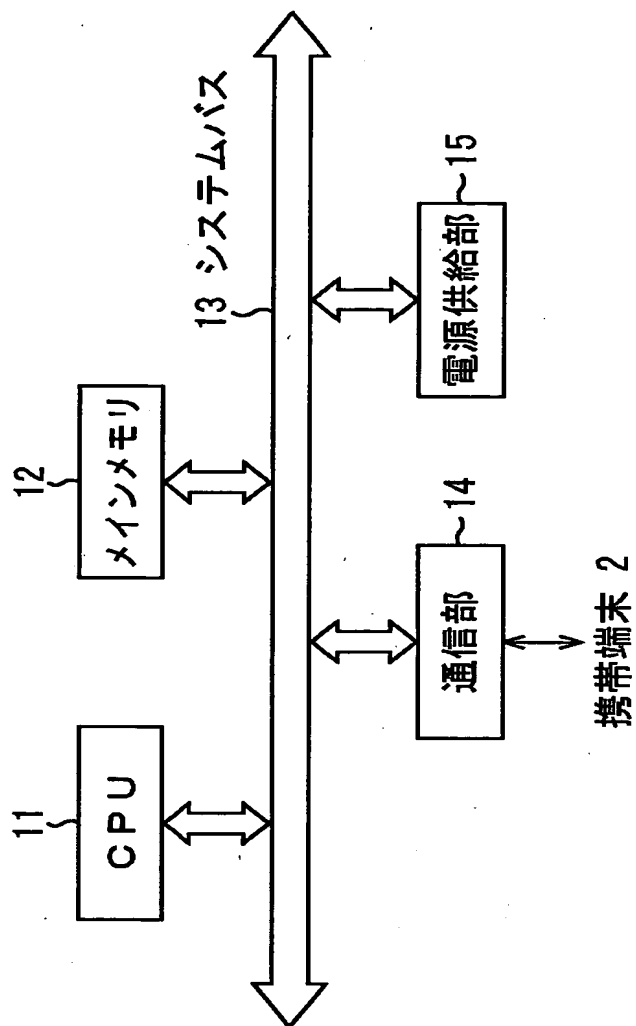
1 腕時計, 2 携帯端末, 3-1 精算装置, 3-2 モニター,
3-3 パーソナルコンピュータ, 3-4 改札機, 3-5 改札機,
3-6 券売機, 3-7 ゲート機, 3-8 通過監視装置, 3-9
通過監視装置, 3-10 入門ゲート機, 3-11 料金ゲート機, 3-
12 精算装置, 3-13 カルテ管理端末, 3-14 携帯電話, 4
ネットワーク, 5 個人サーバ, 6-1 サービスサーバ, 6-2 ショ
ッピングサーバ, 6-3 駅サーバ, 6-4 駅サーバ, 6-5 チケッ
トサーバ, 6-6 ゲートサーバ, 6-7 監視サーバ, 6-8 通行料
金サーバ, 6-9 公共料金サーバ, 6-10 カルテ管理サーバ, 6-
11 計算サーバ, 11 CPU, 12 メインメモリ, 13 システム
バス, 14 通信部, 15 電源供給部, 21 CPU, 22 メイン
メモリ, 23 入力部, 24 表示部, 25 出力部, 26 通信部,
27 通信部, 28 インターフェース, 31 CPU, 32 ROM
, 33 RAM, 34 入力部, 35 表示部, 36 ハードディスク
, 37 通信部, 38 通信部, 39 インターフェース, 41 CP
U, 42 ROM, 43 RAM, 44 入力部, 45 表示部,
46 ハードディスク, 47 通信部, 48 インターフェース, 51
指紋採取センサ, 52 マイクロフォン, 61 イメージセンサ, 71
管理サーバ

【書類名】 図面

【図 1】

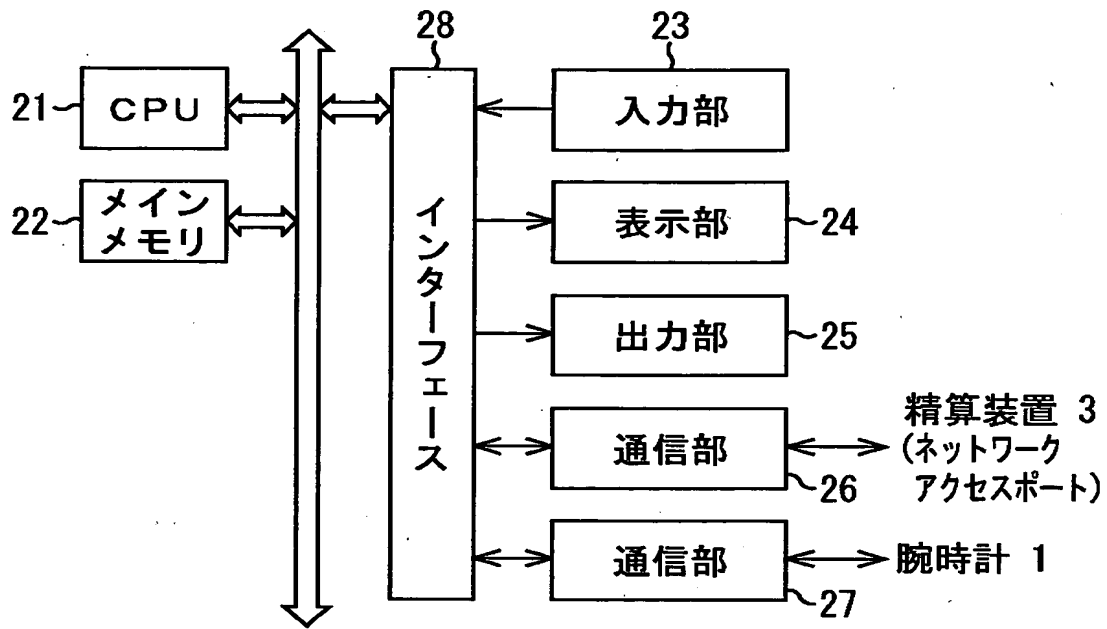


【図 2】



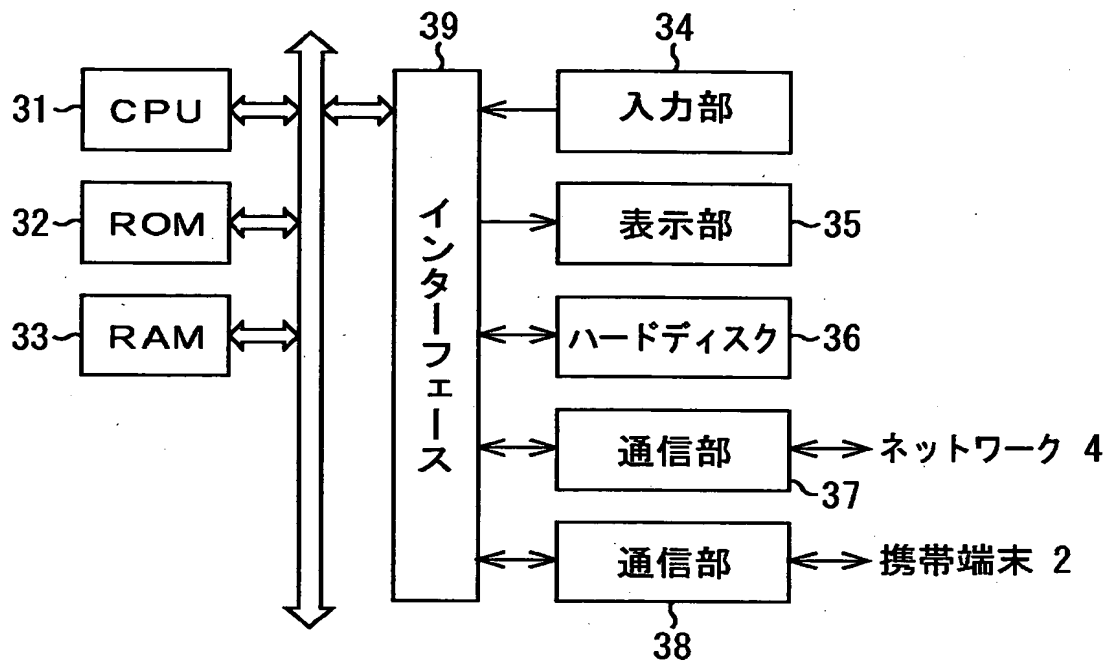
腕時計 1 (認証データ用ICチップ)

【図 3】



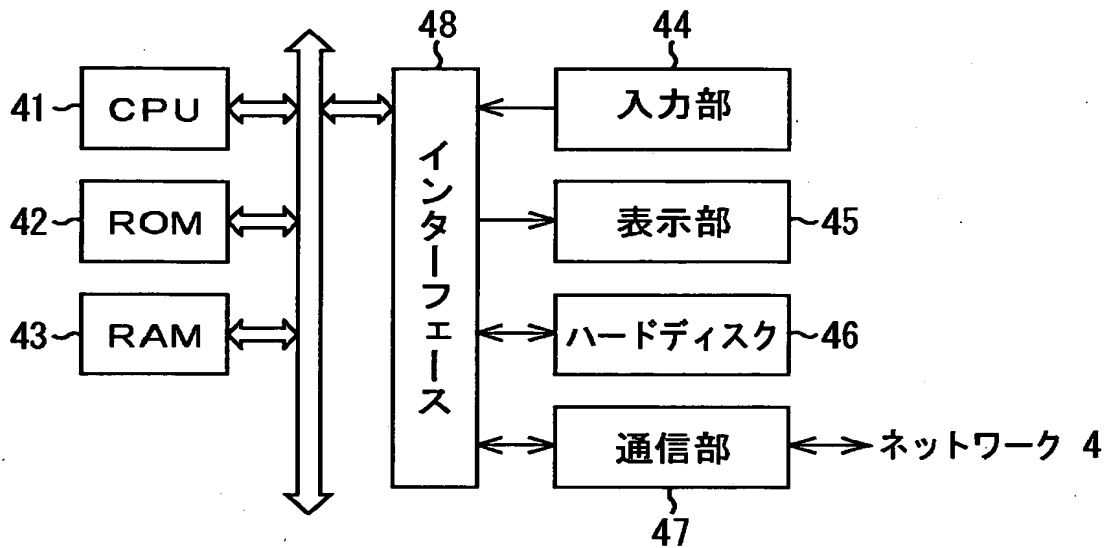
携帯端末 2

【図 4】



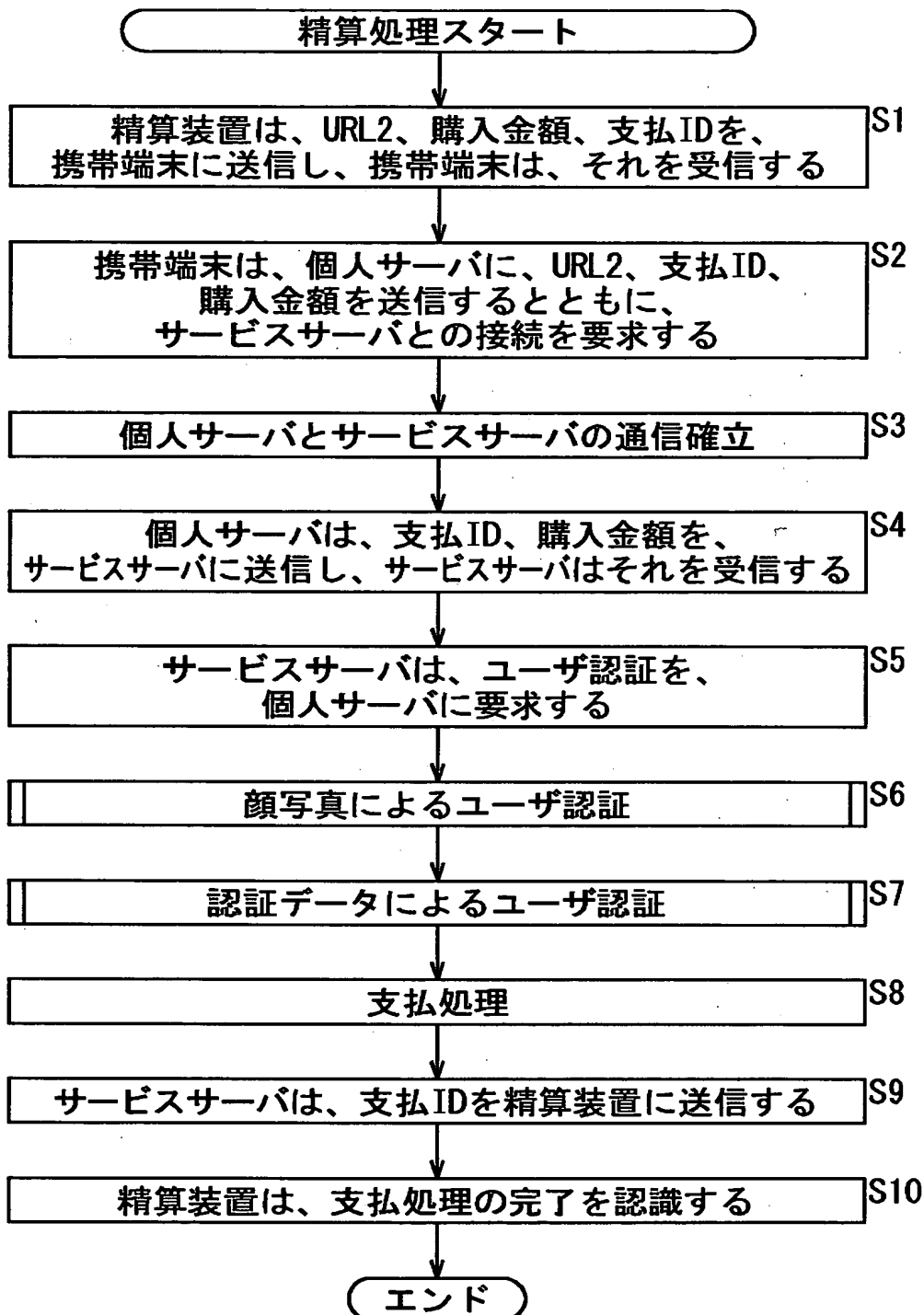
精算装置 3-1

【図5】

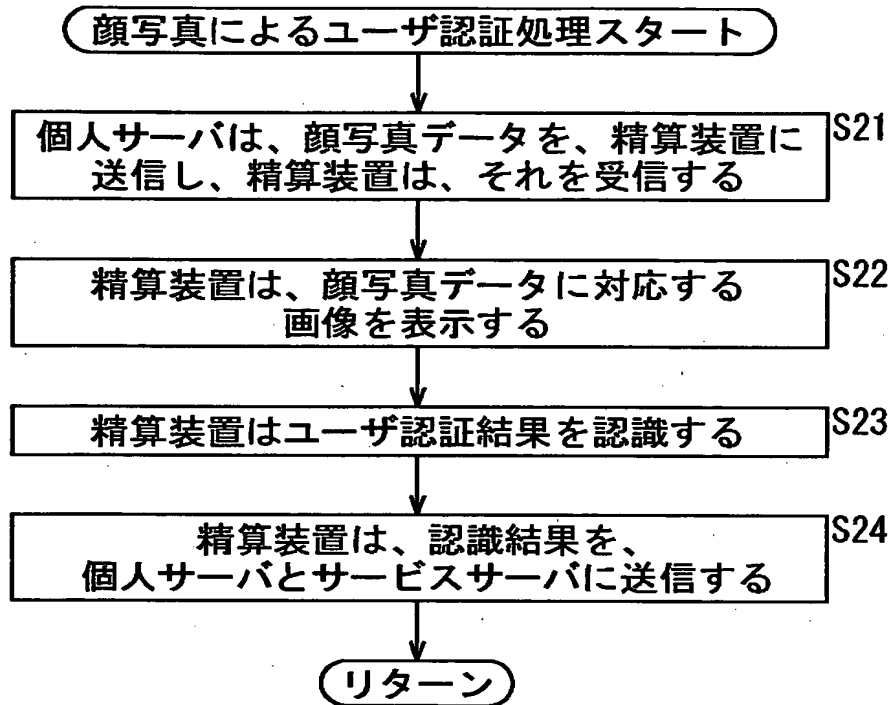


個人サーバ 5

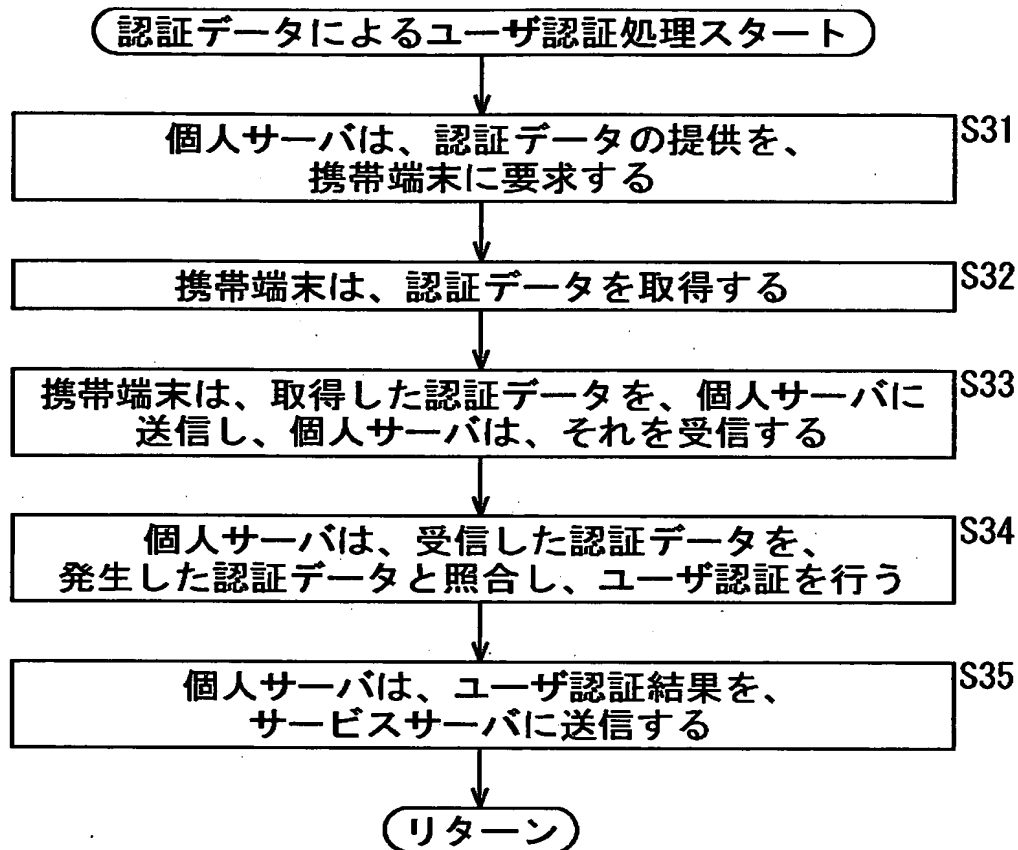
【図 6】



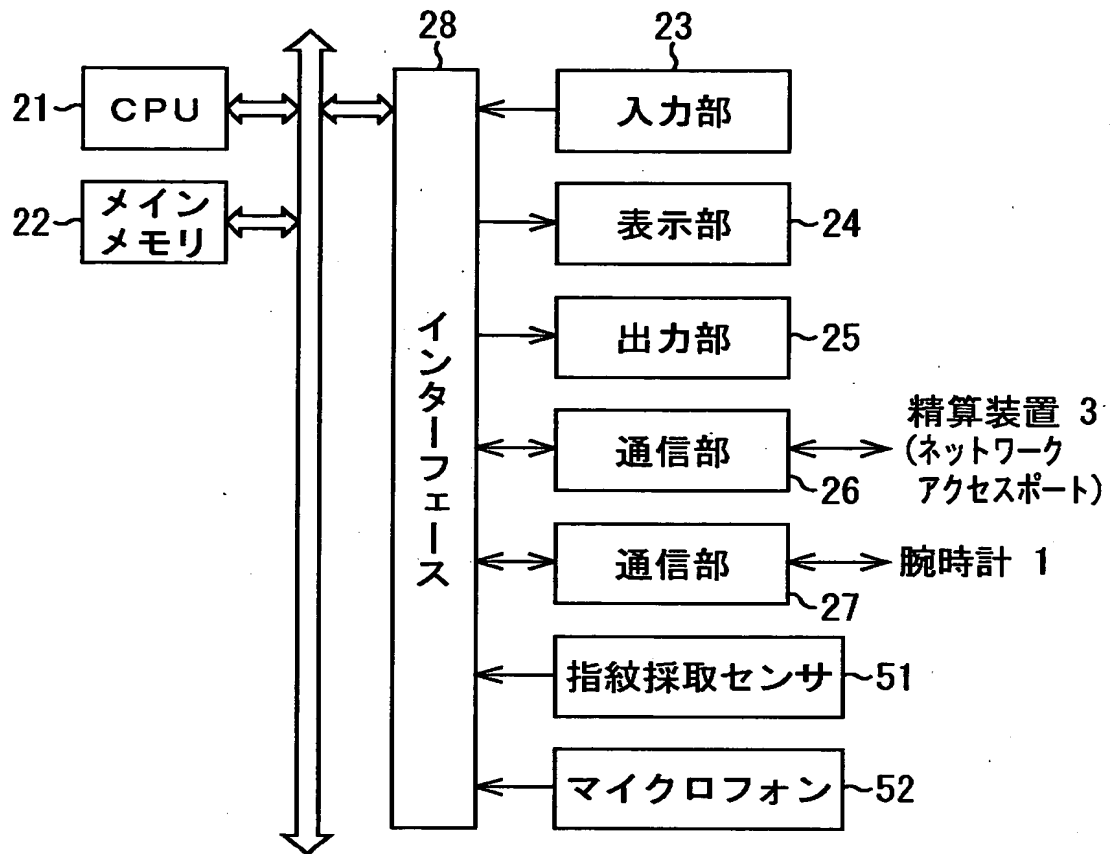
【図 7】



【図 8】

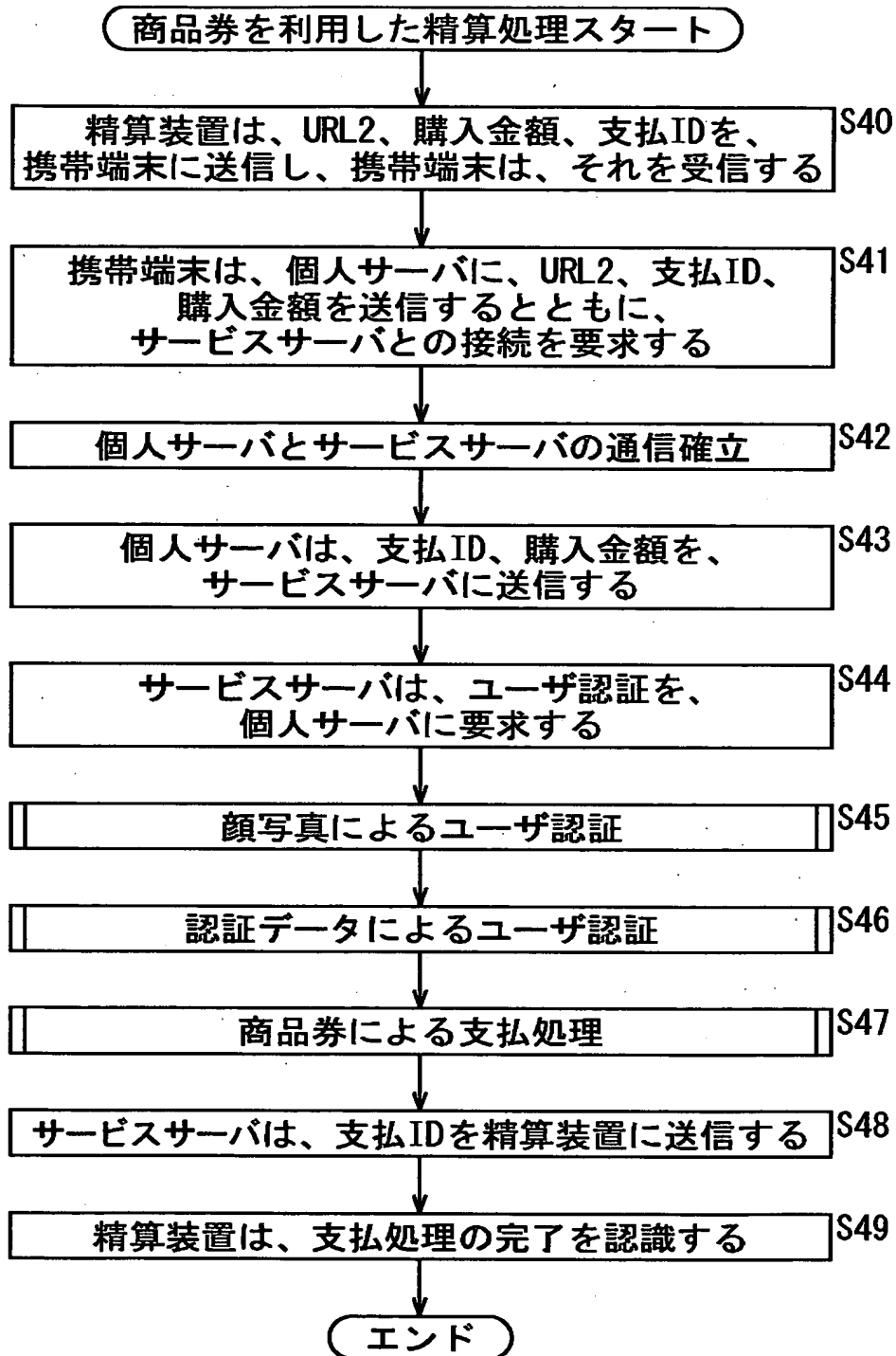


【図 9】

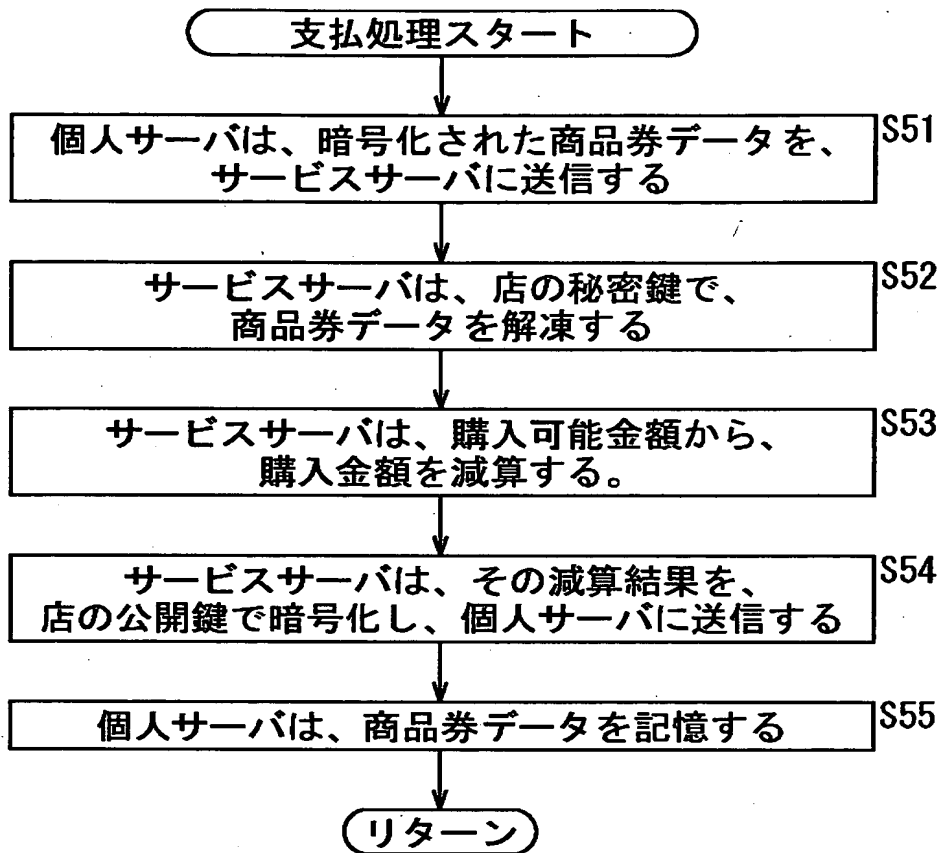


携帯端末 2

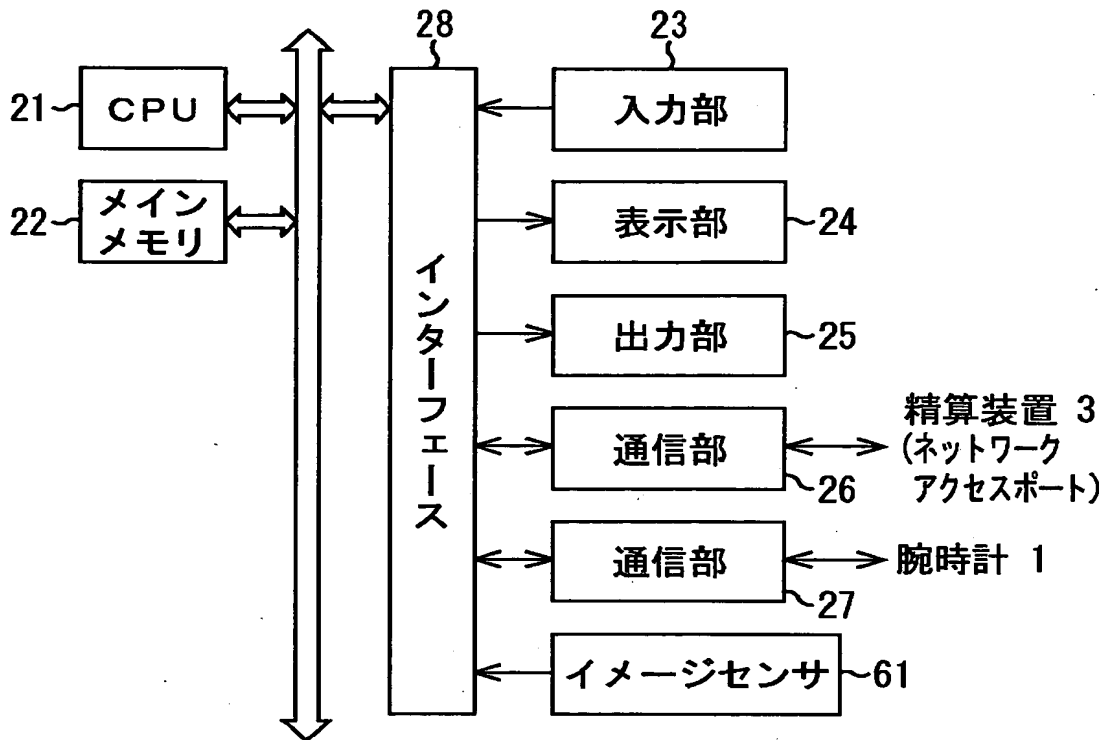
【図 1 0】



【図11】

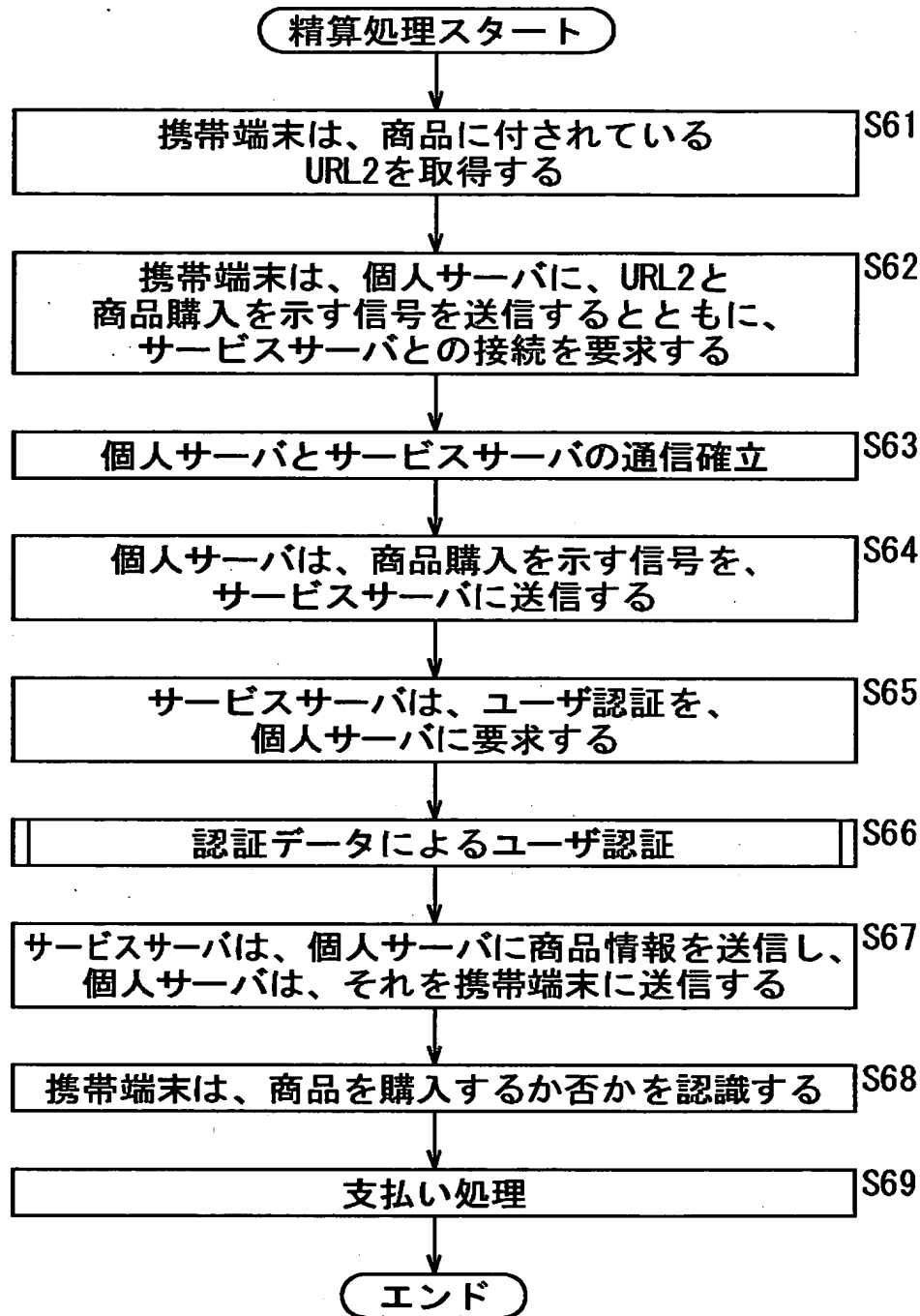


【図12】

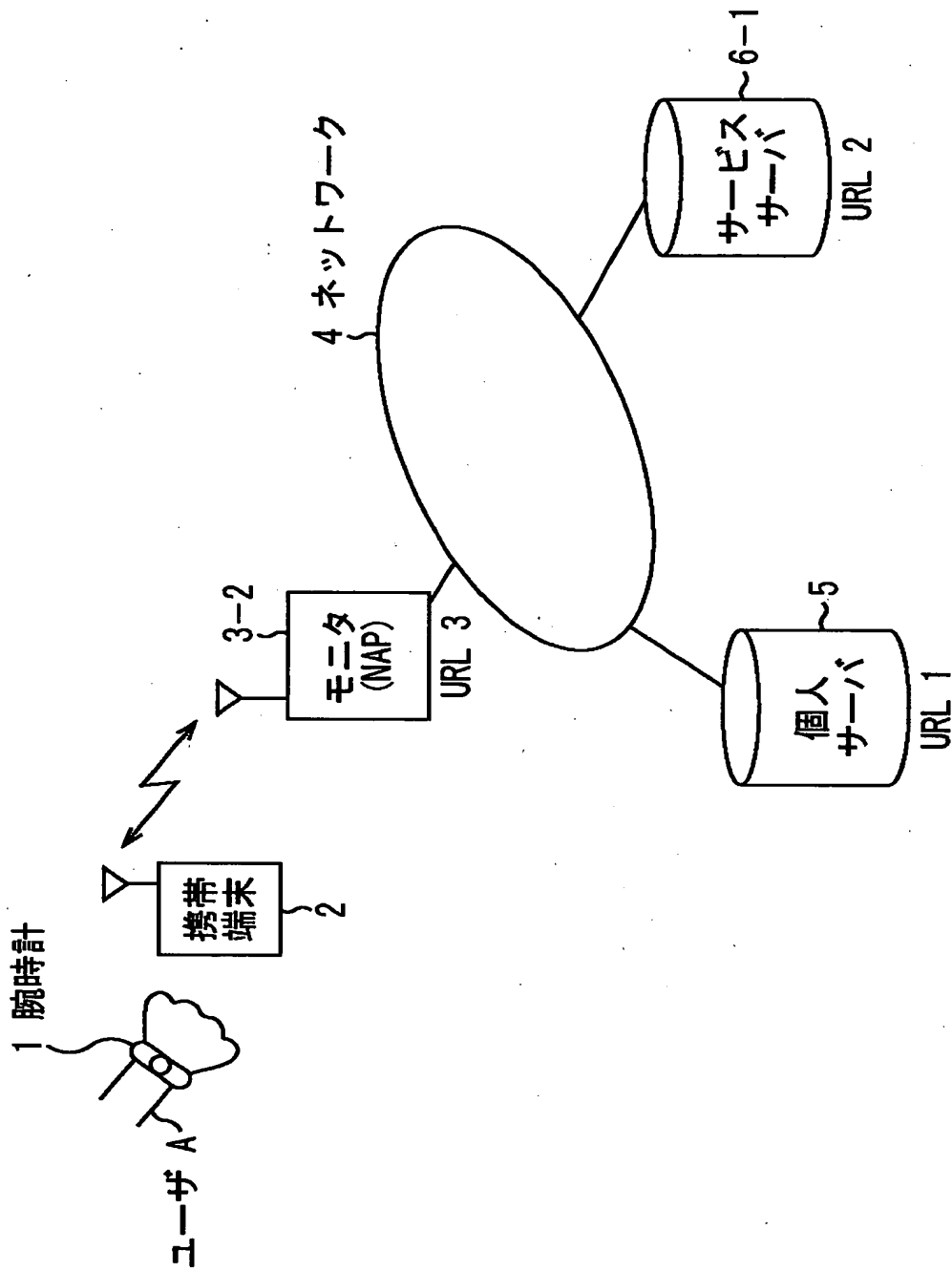


携帯端末 2

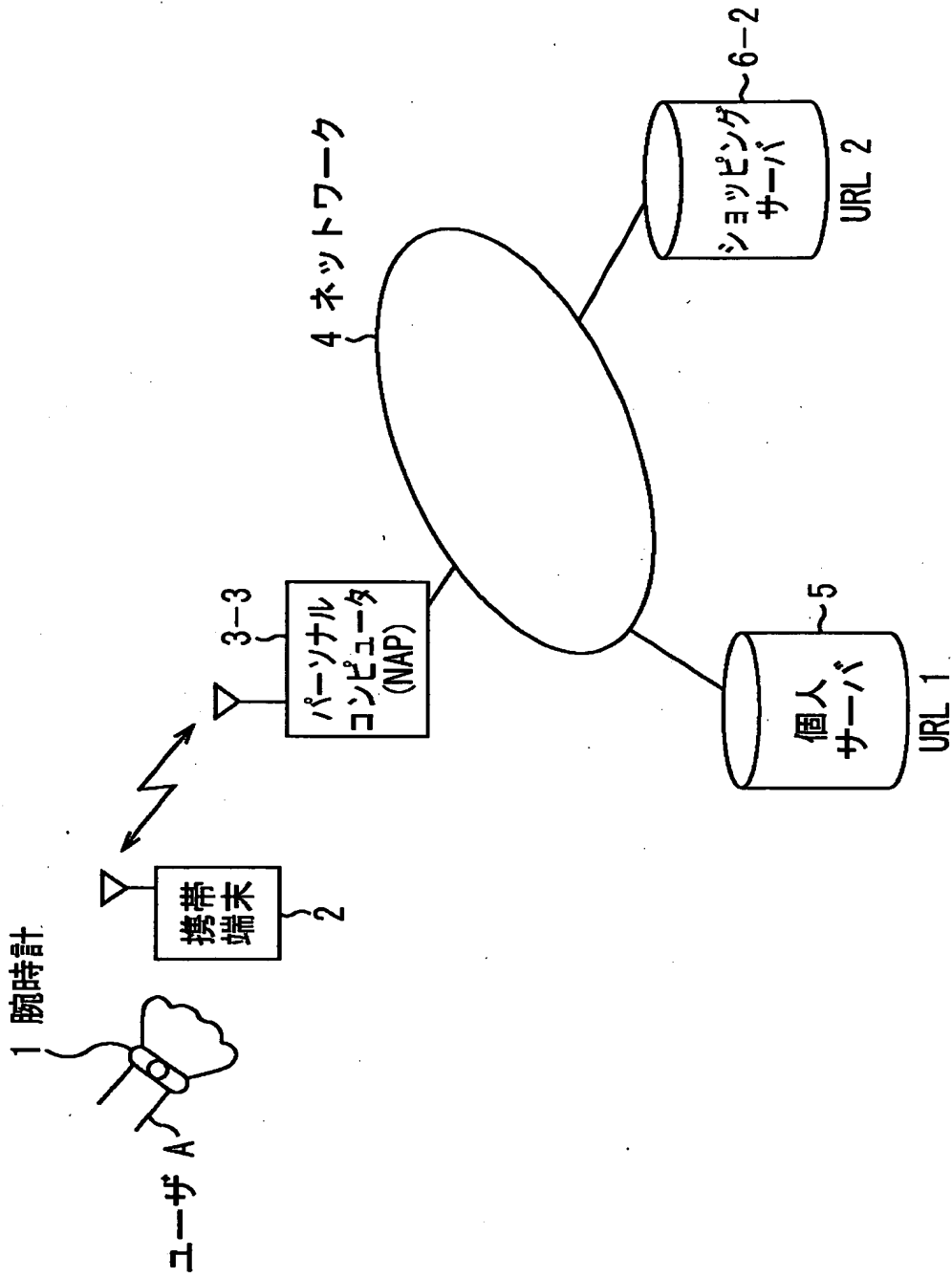
【図 13】



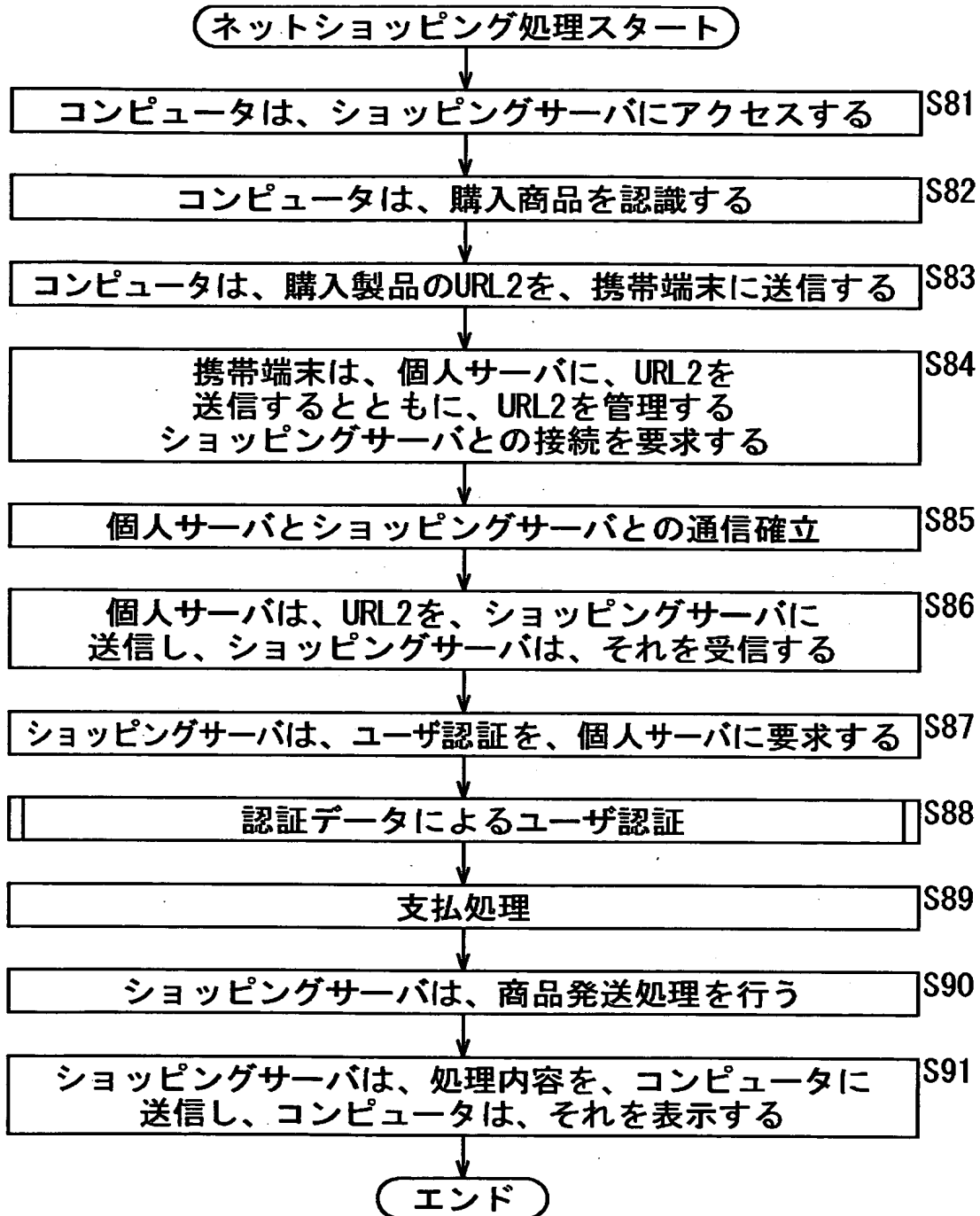
【図 14】



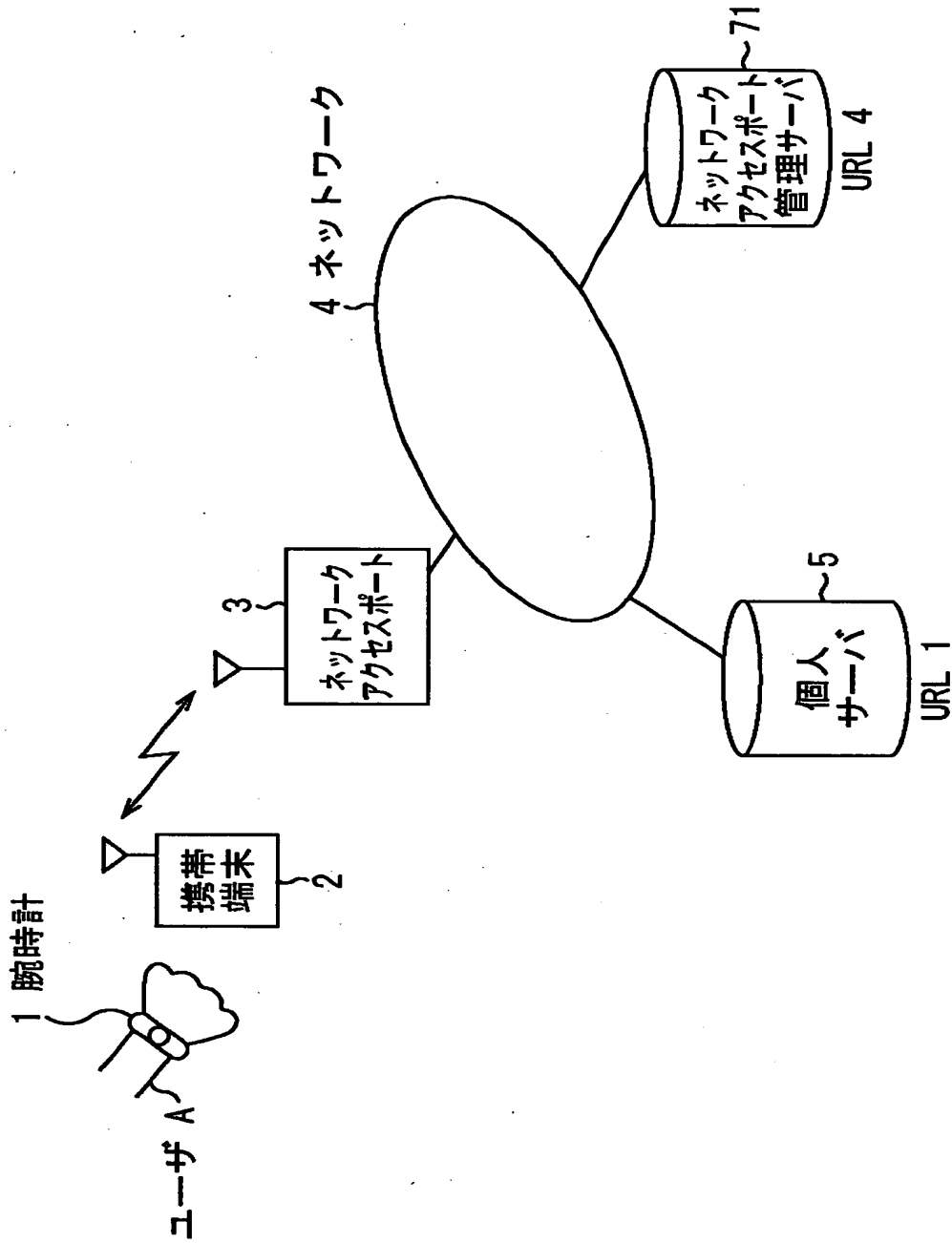
【図 1 5】



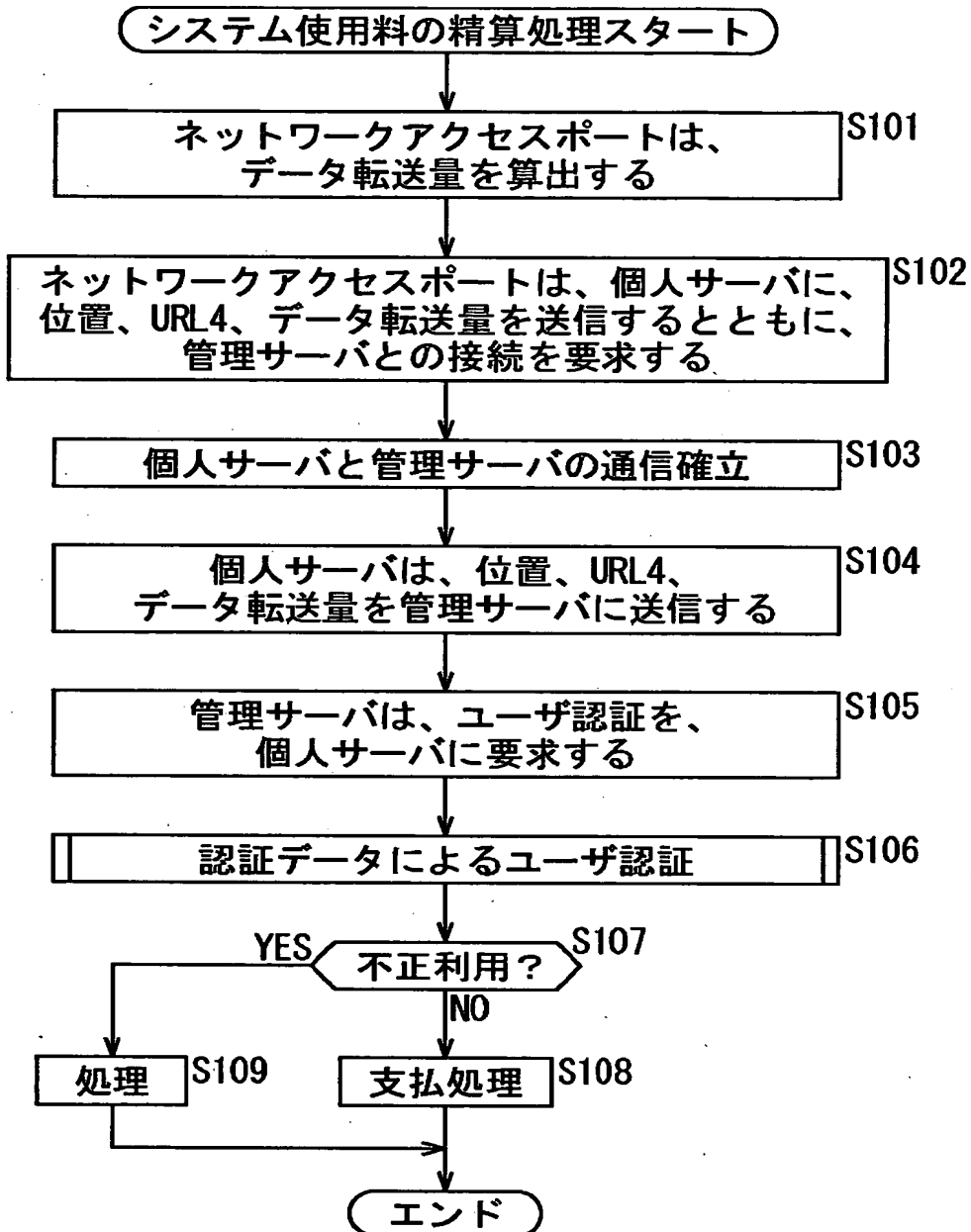
【図 16】



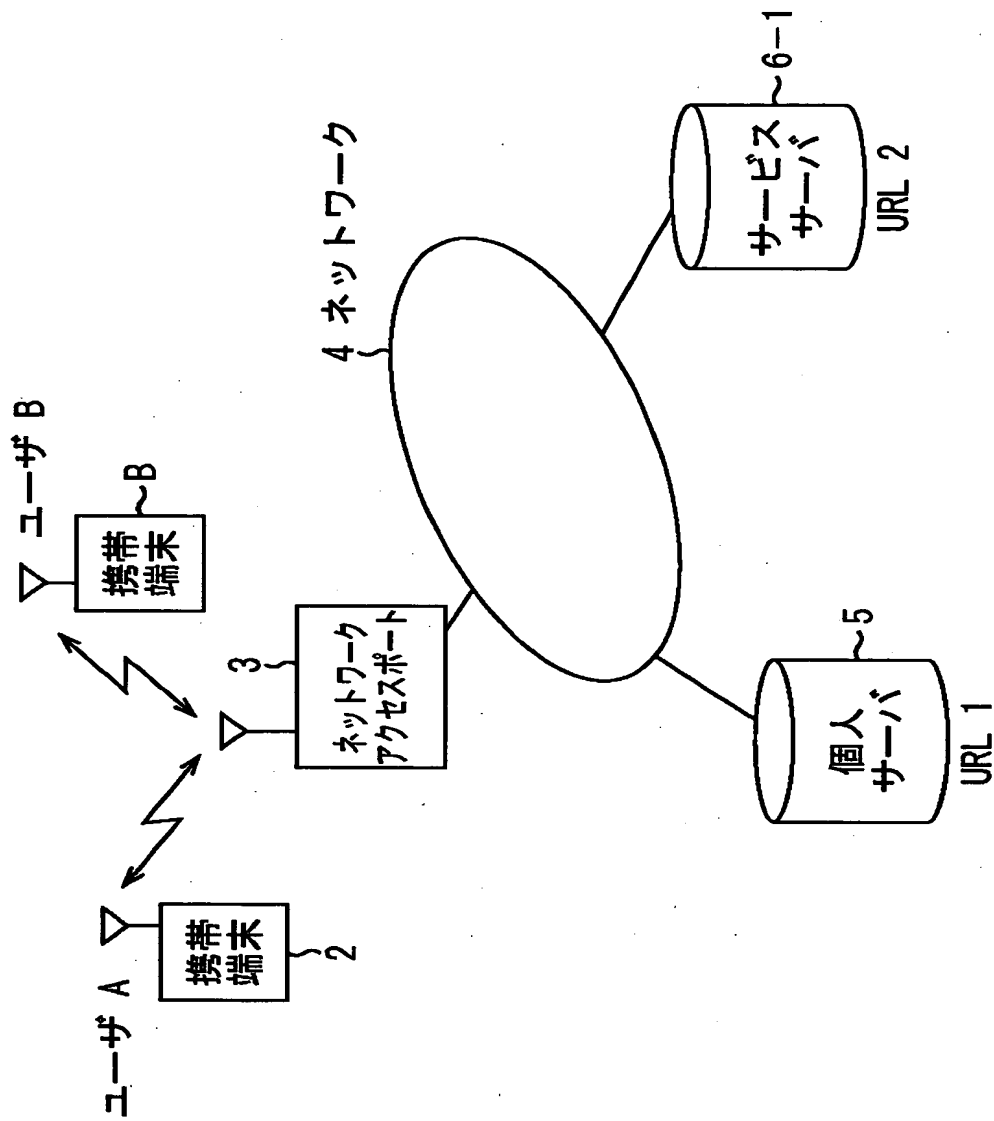
【図17】



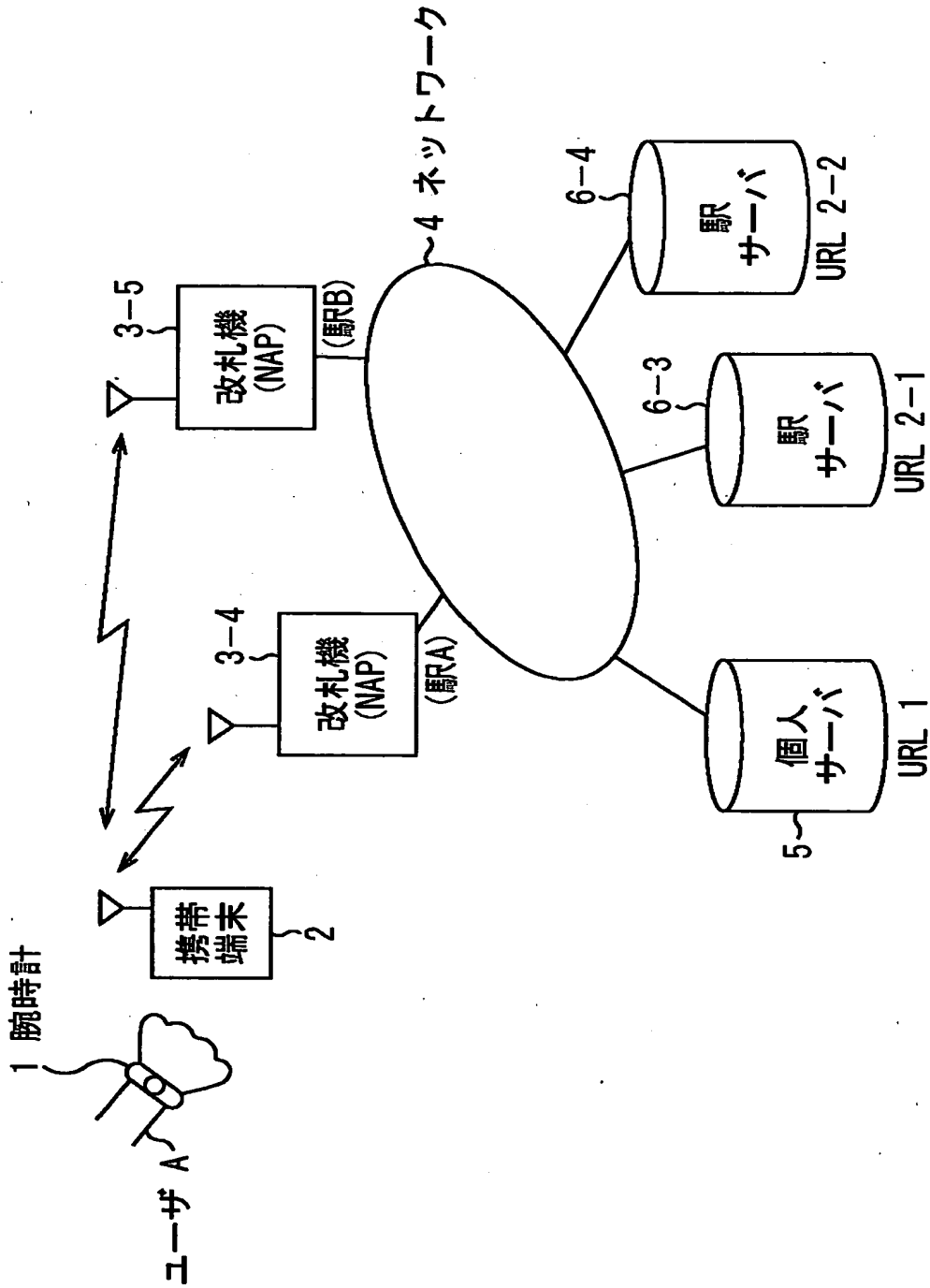
【図18】



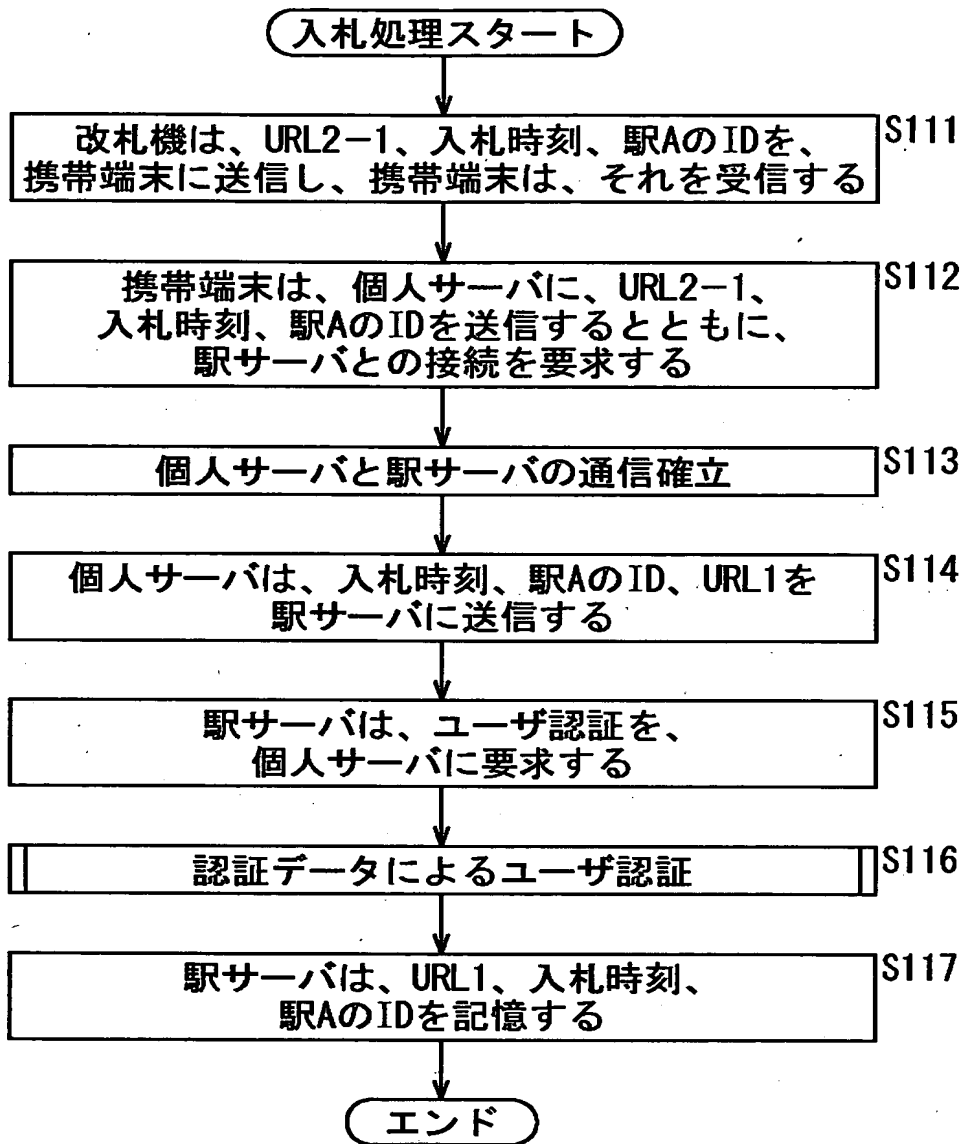
【図19】



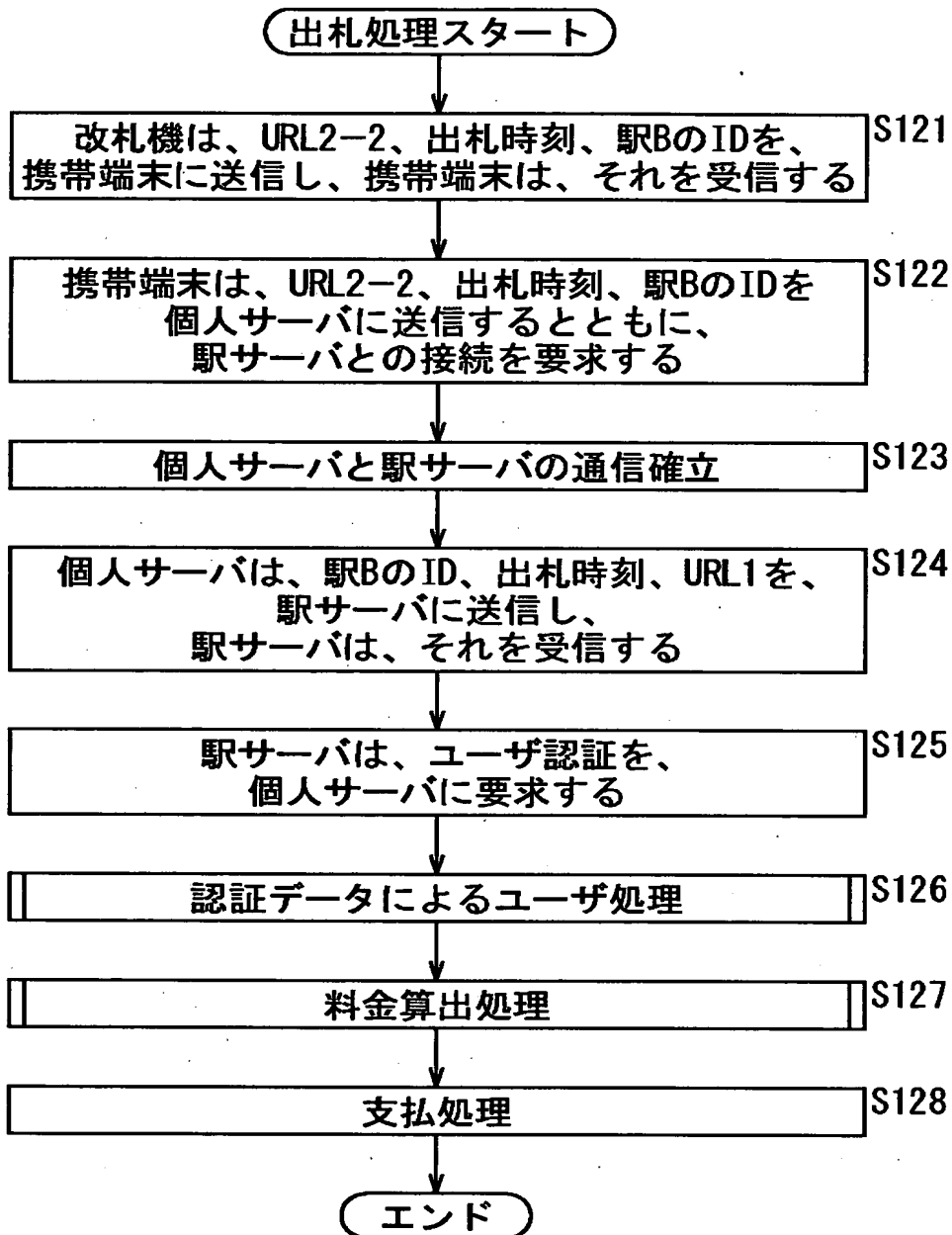
【図 20】



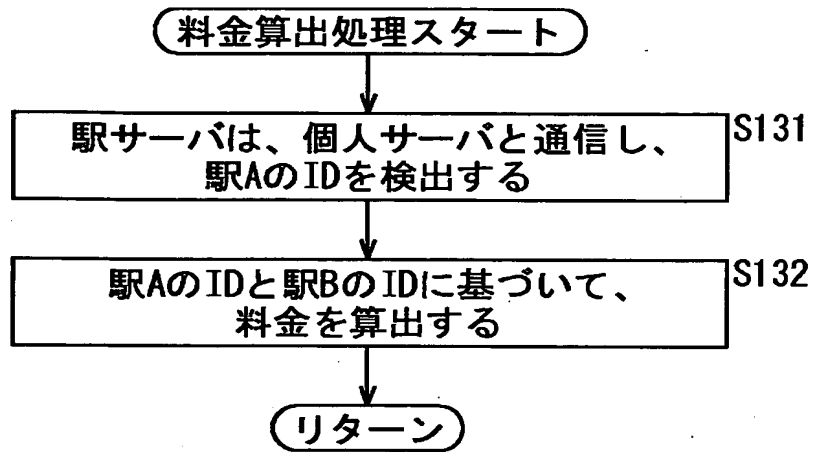
【図 2 1】



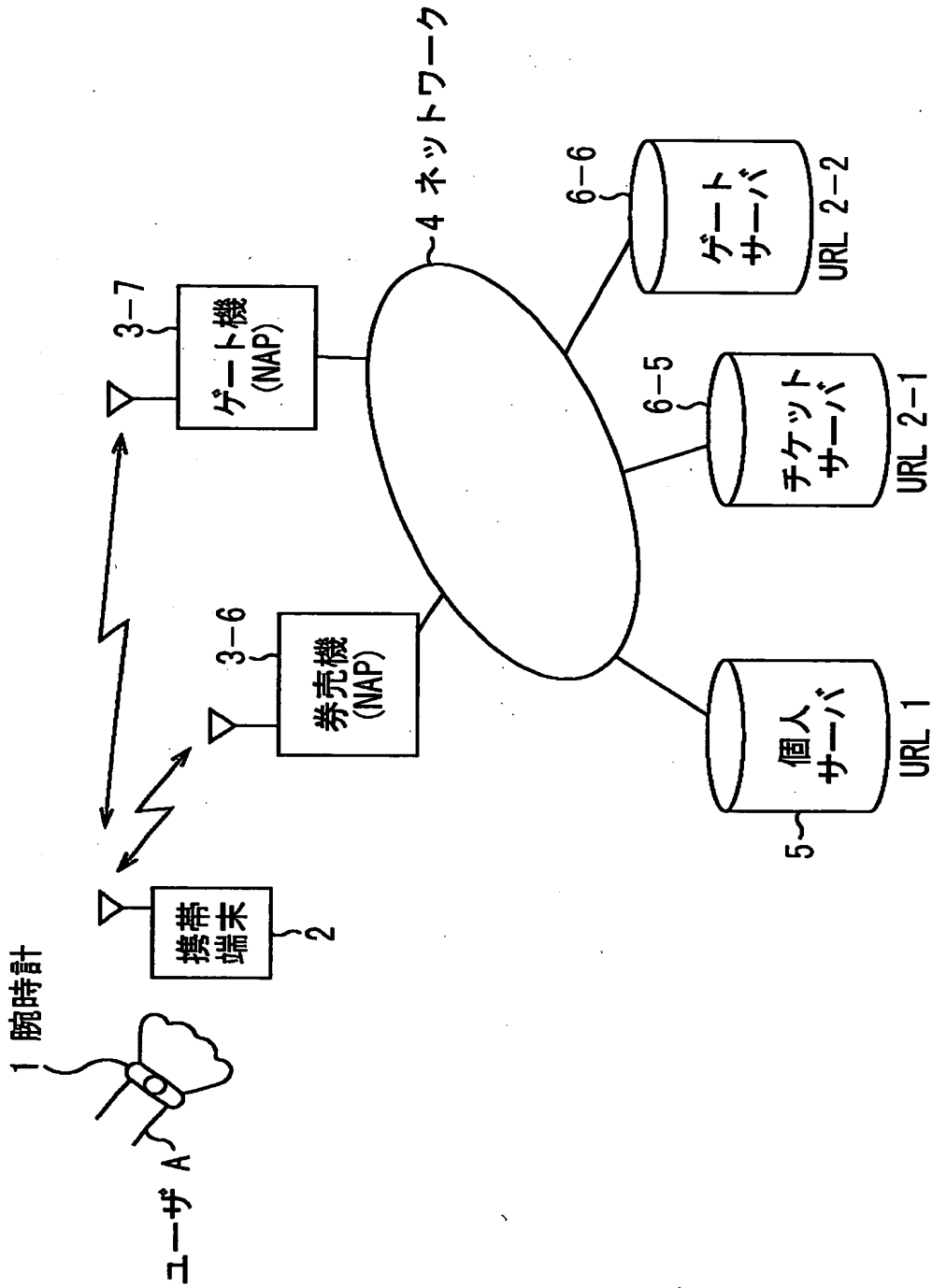
【図 2 2】



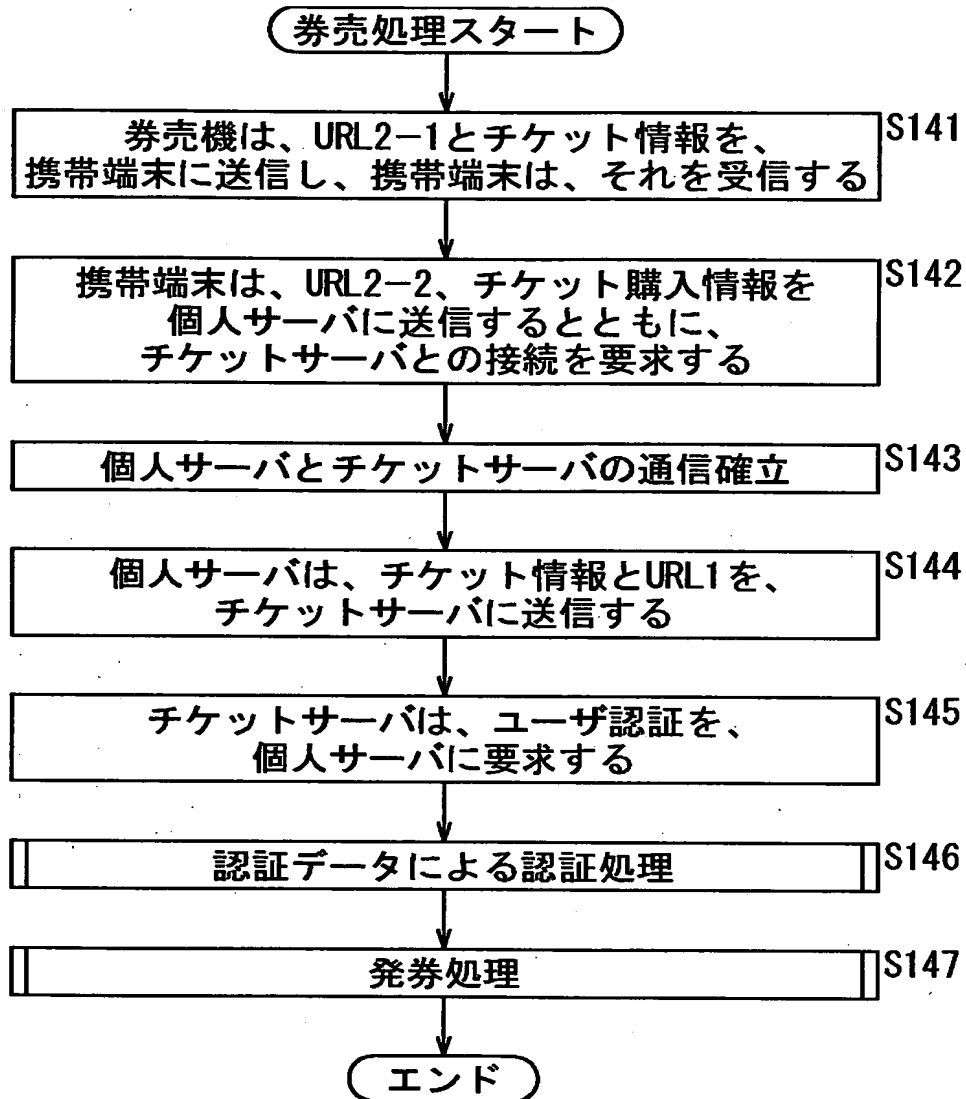
【図 2 3】



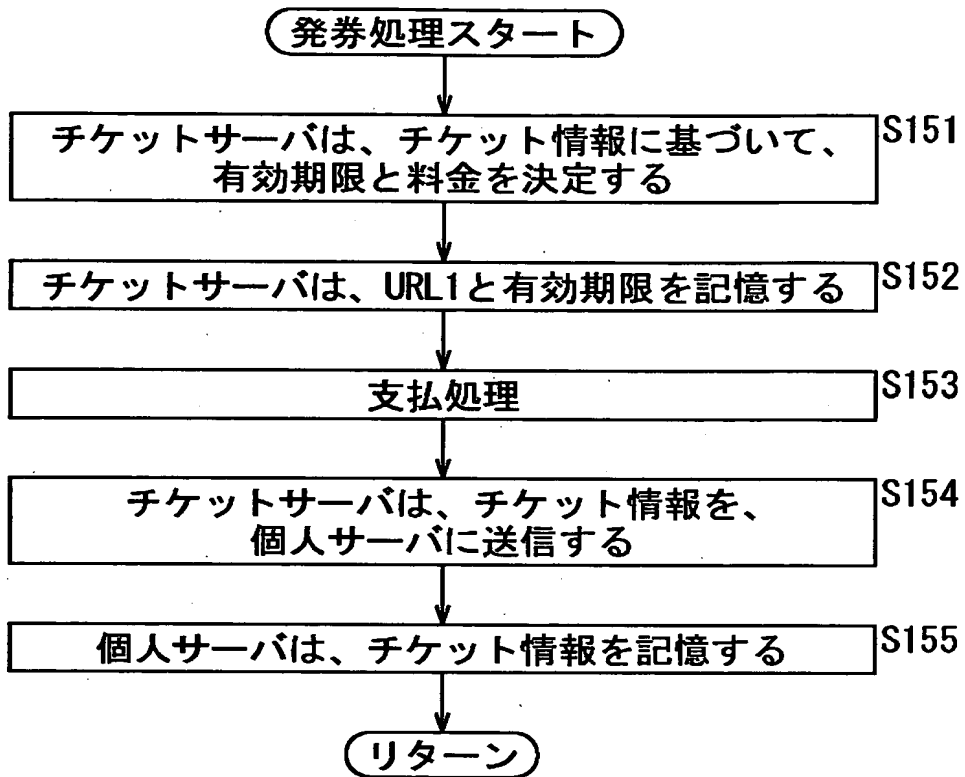
【図 24】



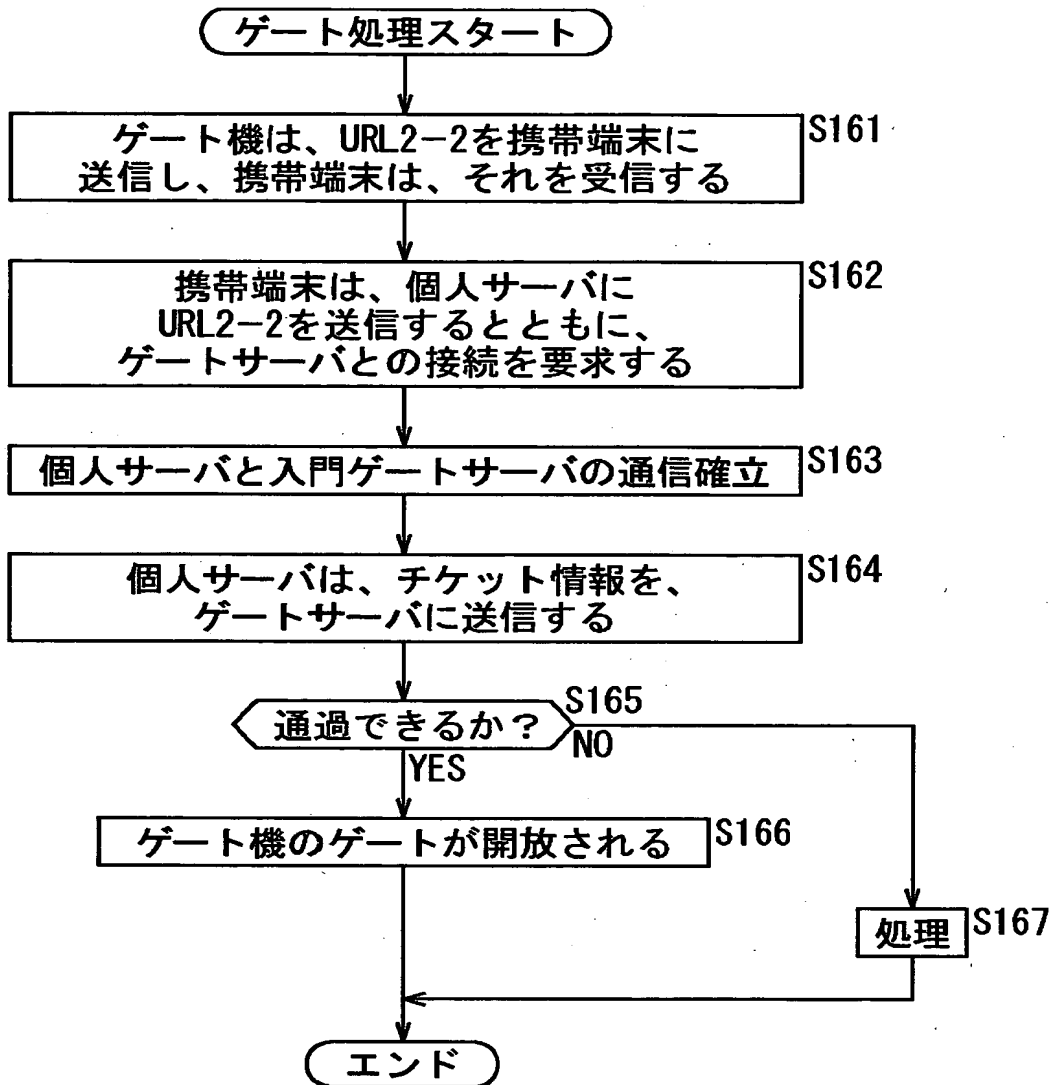
【図 25】



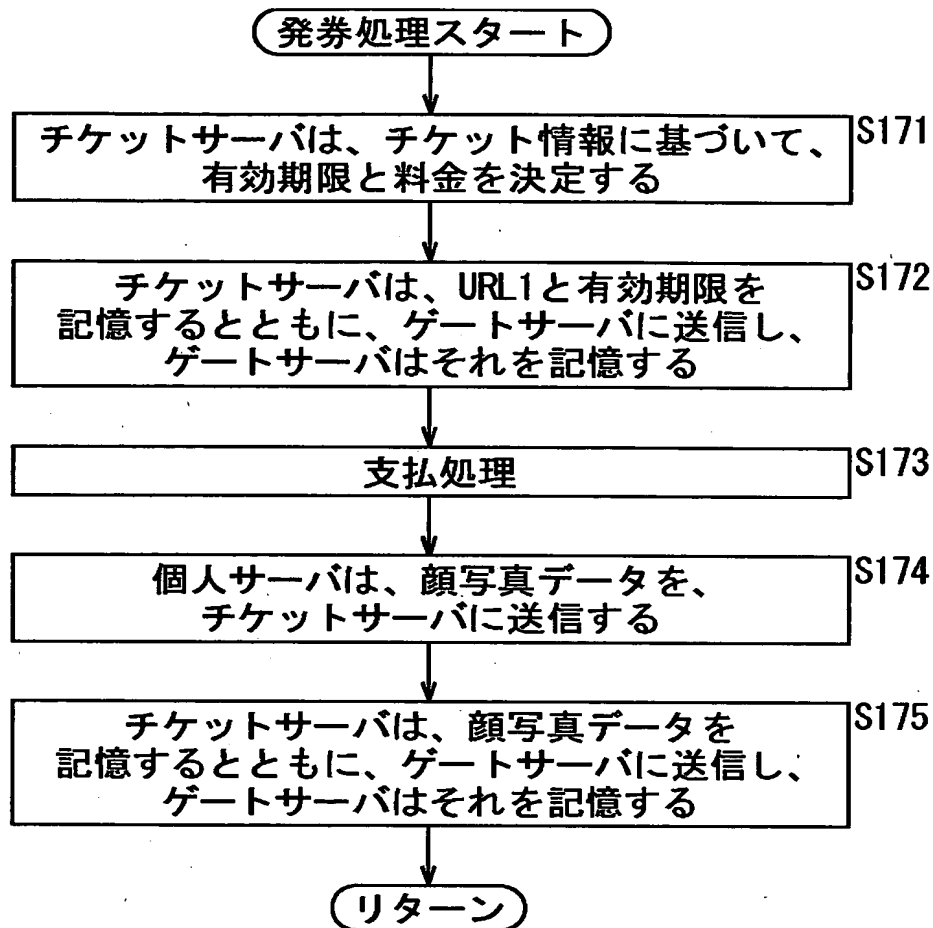
【図 2 6】



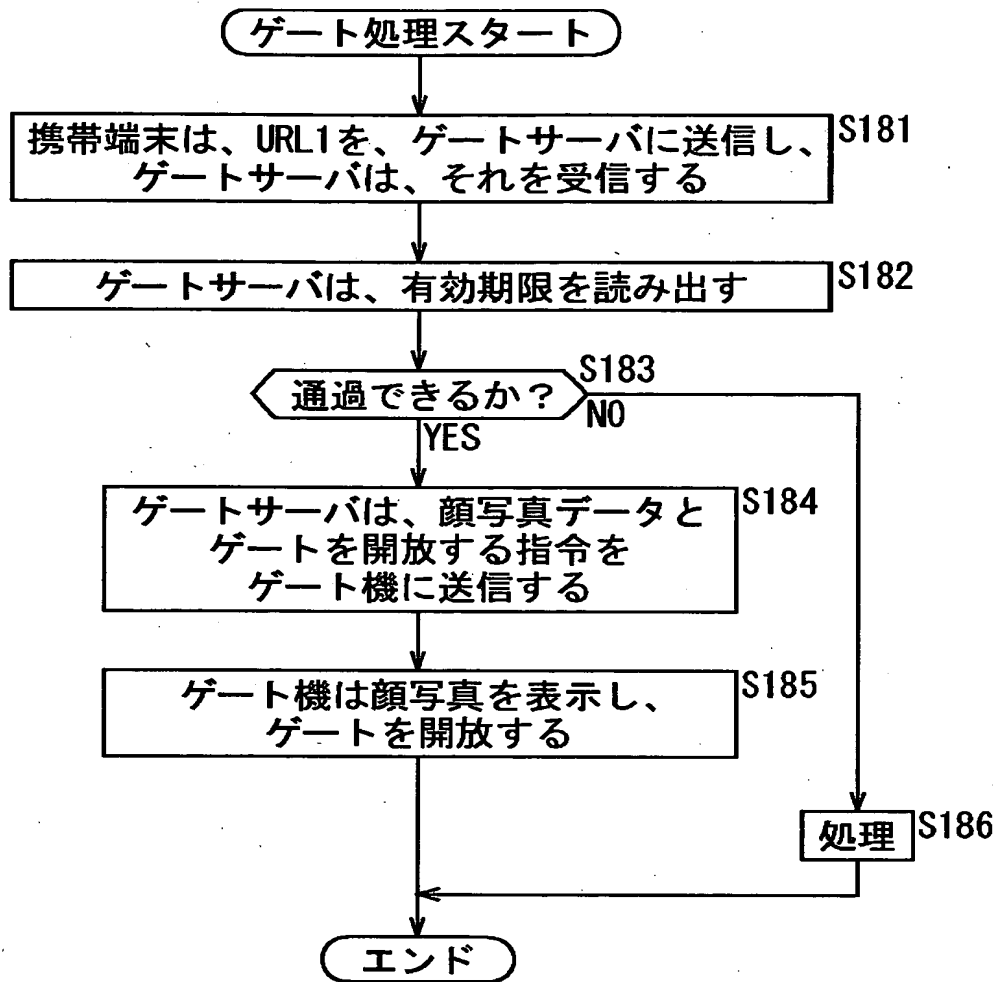
【図 2 7】



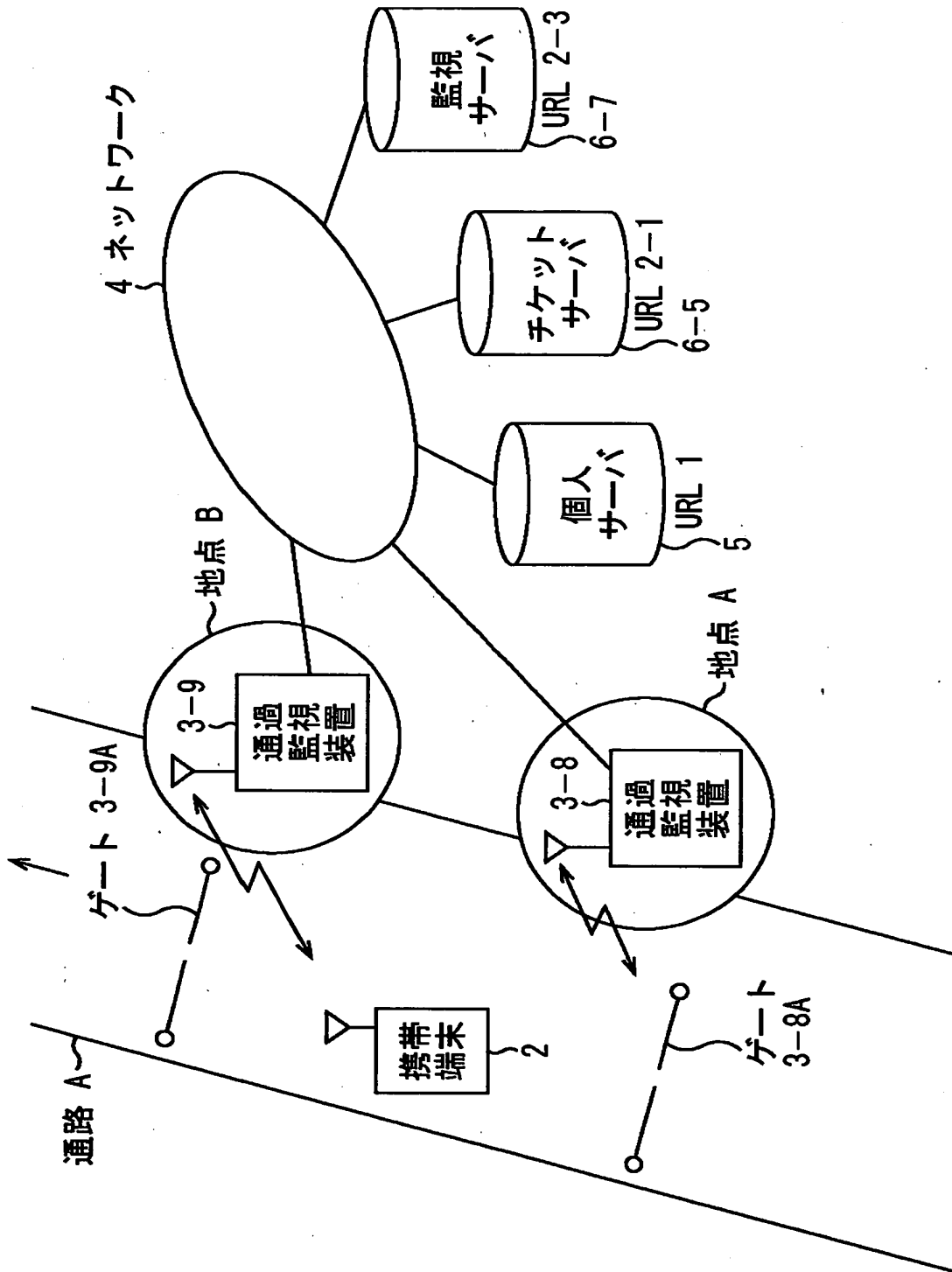
【図 2 8】



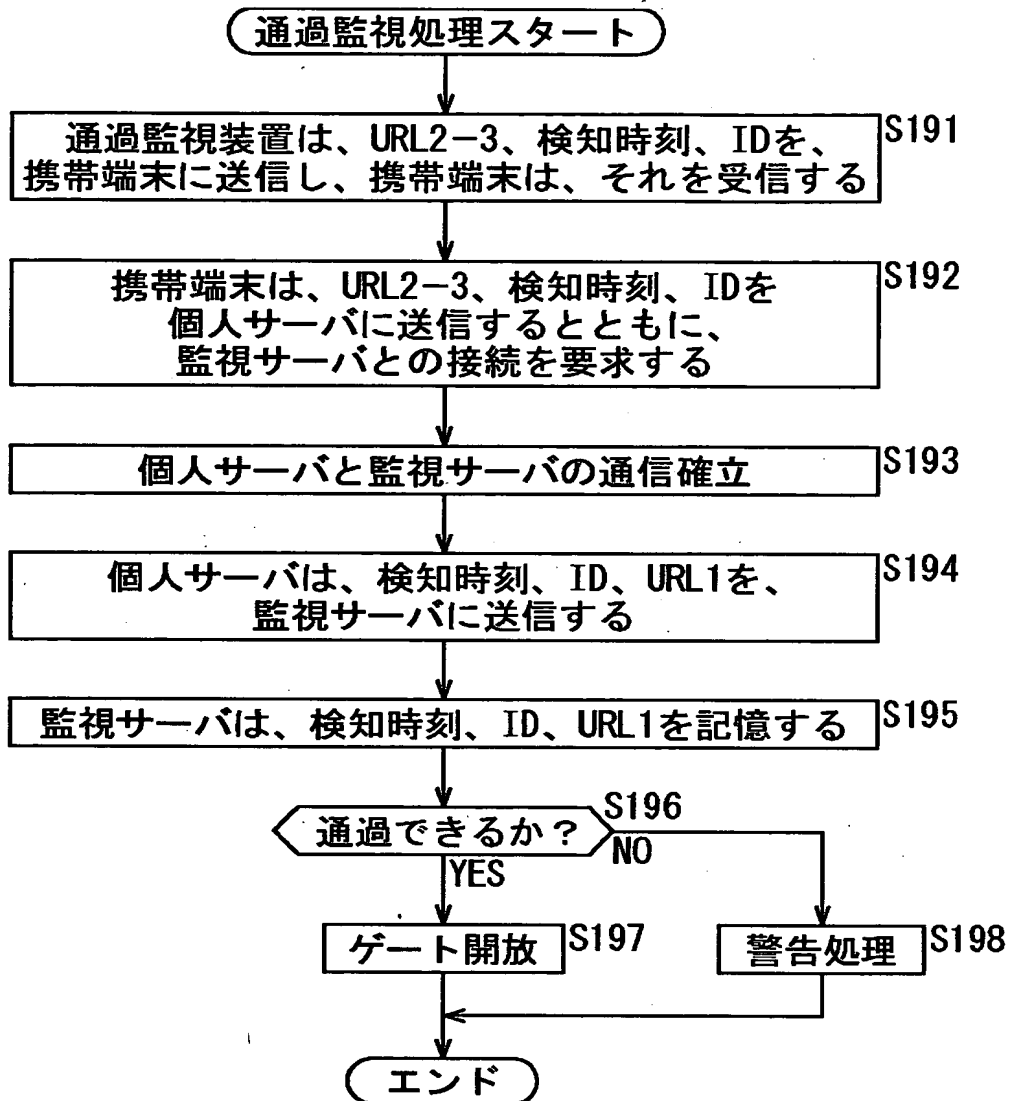
【図 2 9】



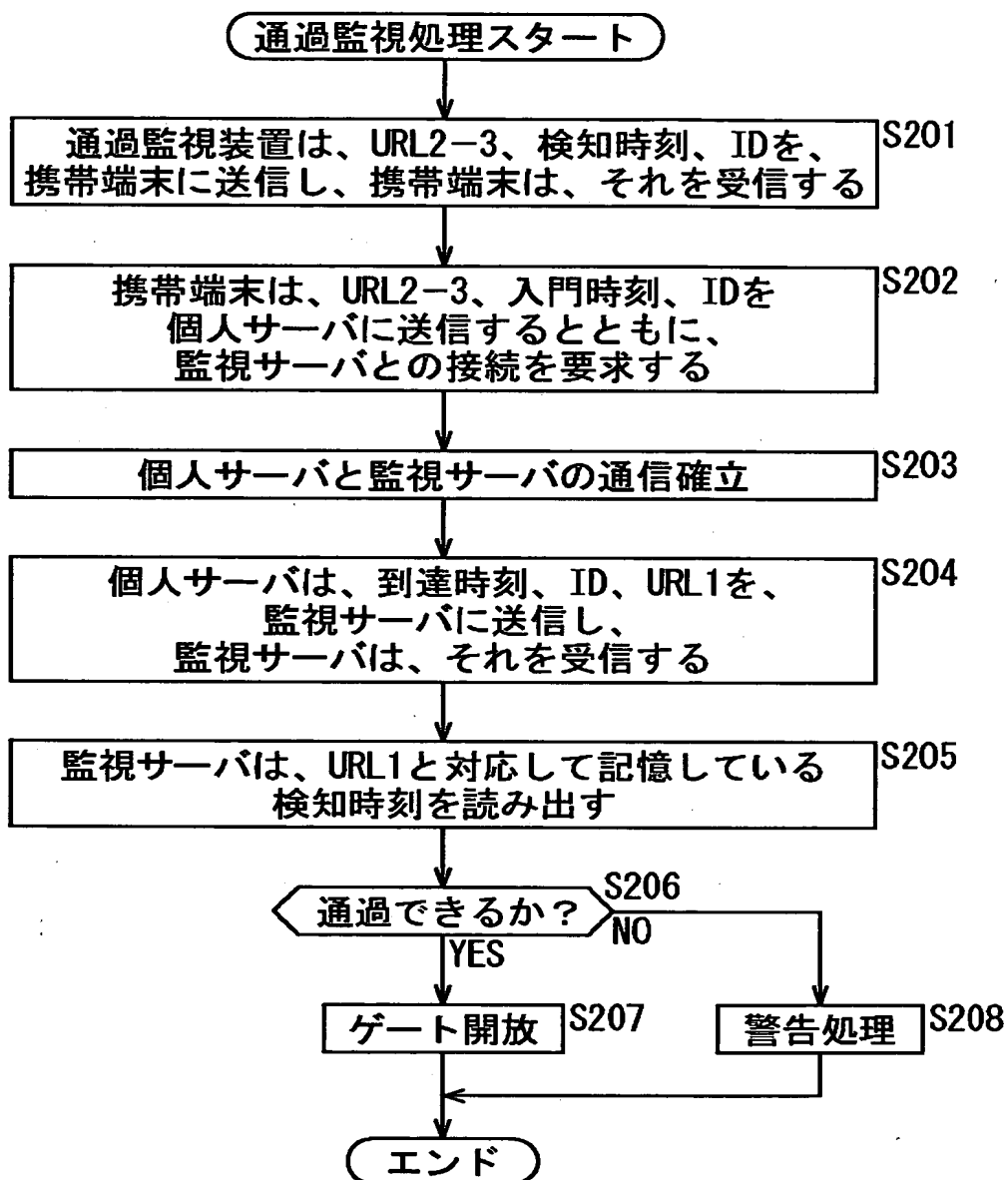
【図 30】



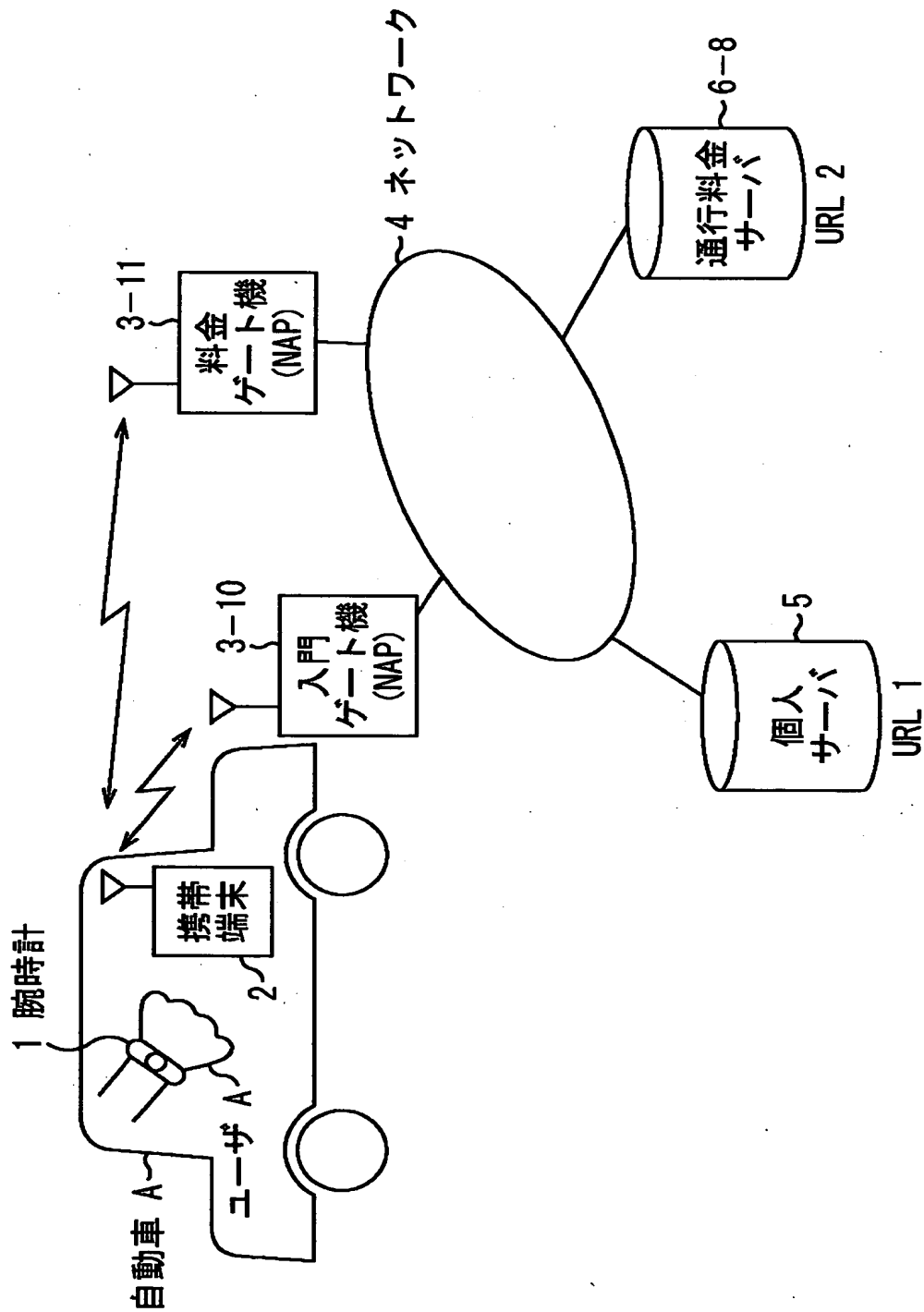
【図 3 1】



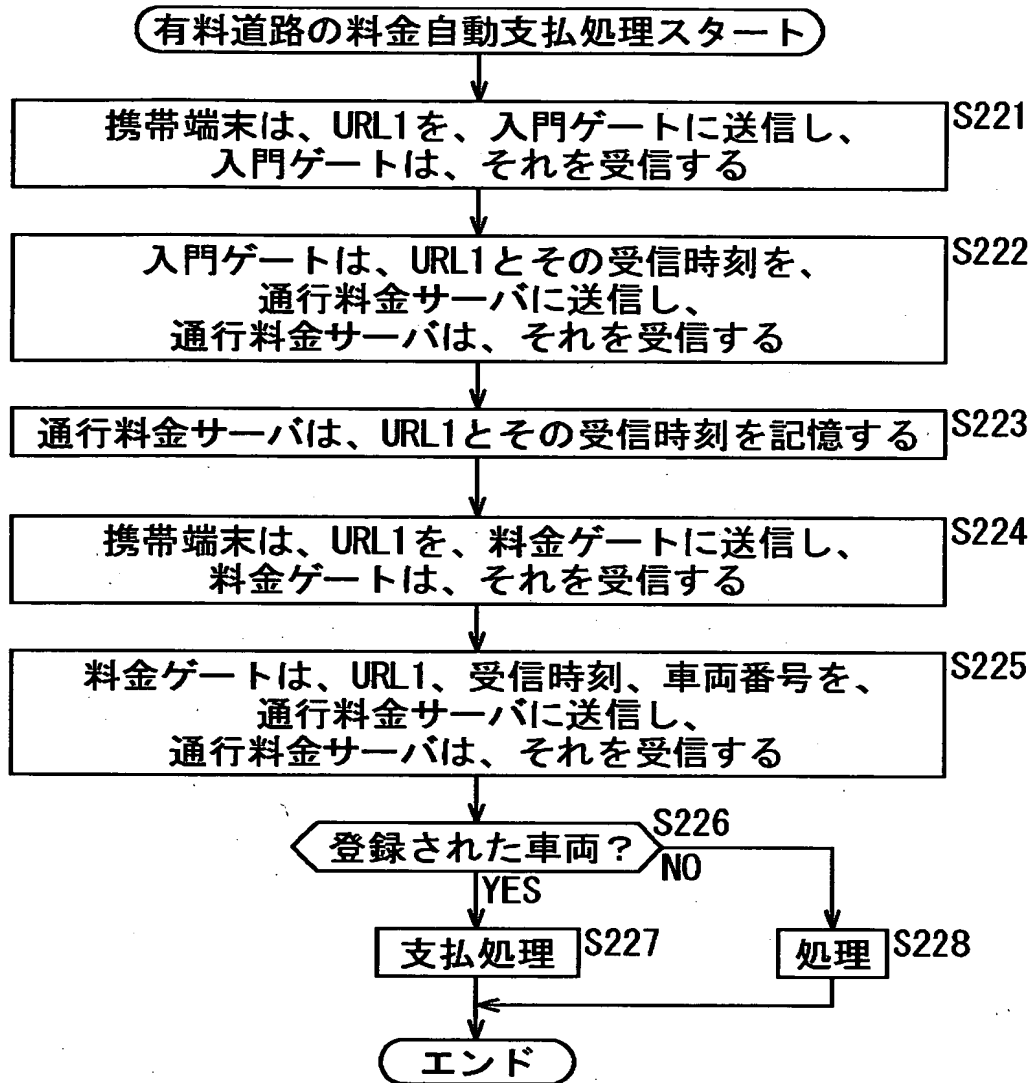
【図 3 2】



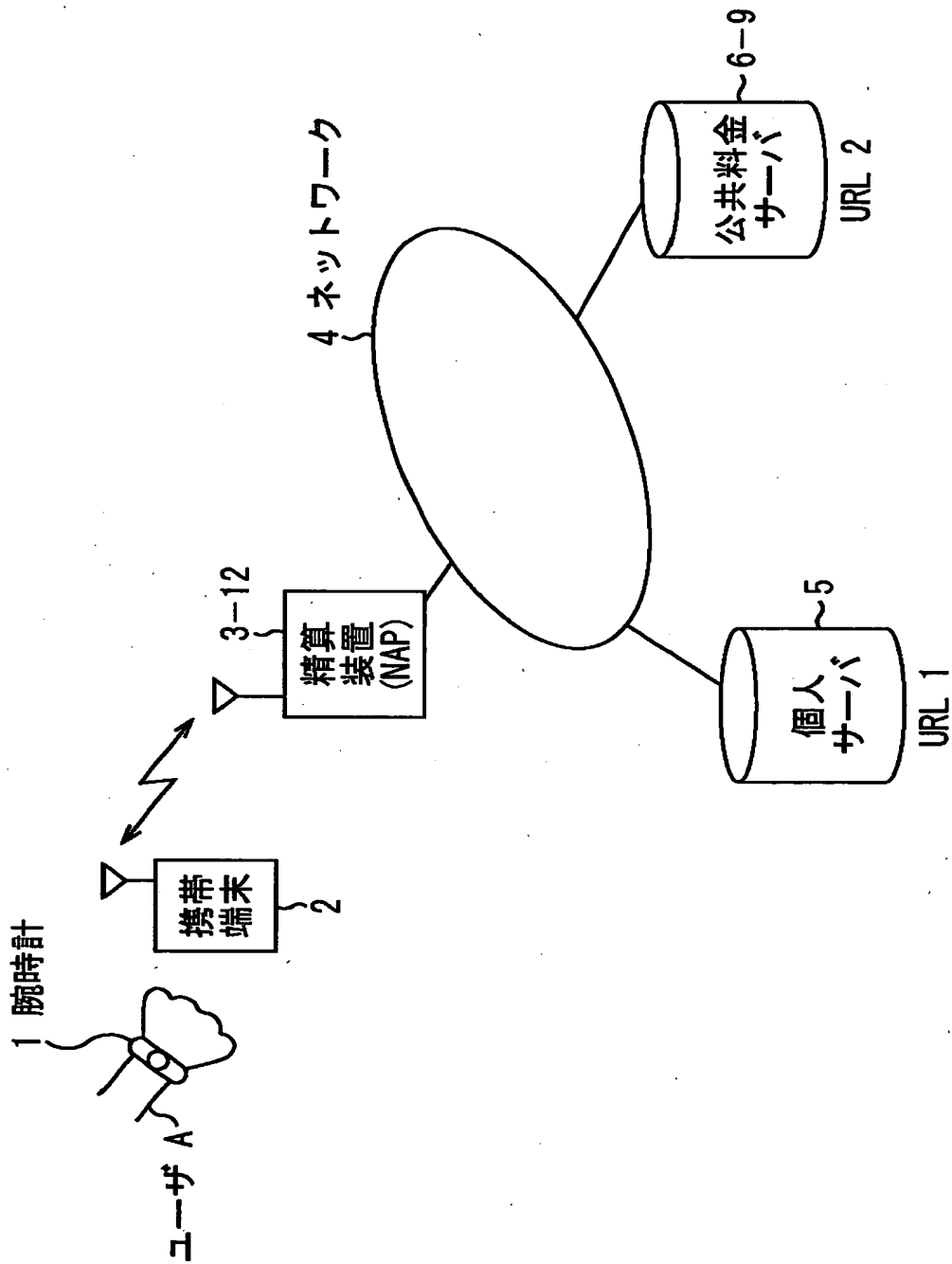
【図 33】



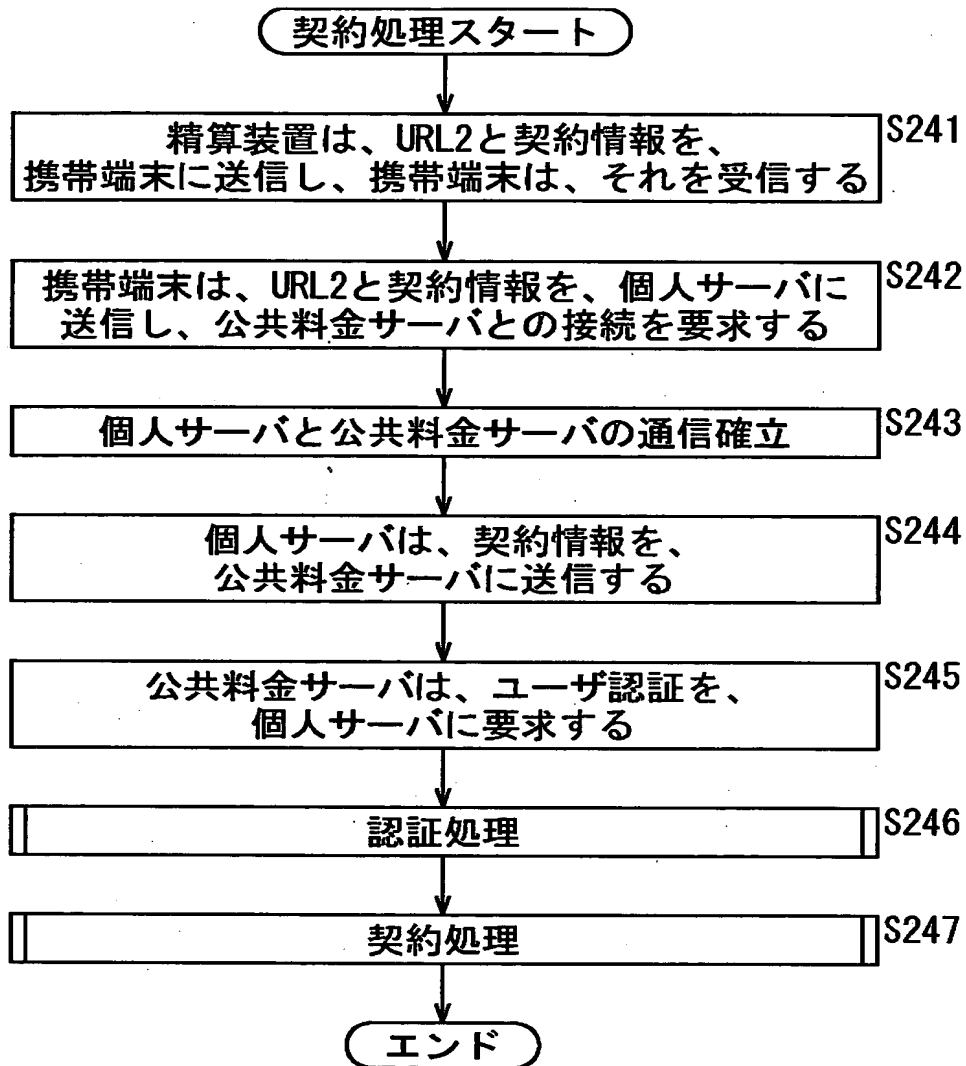
【図 3 4】



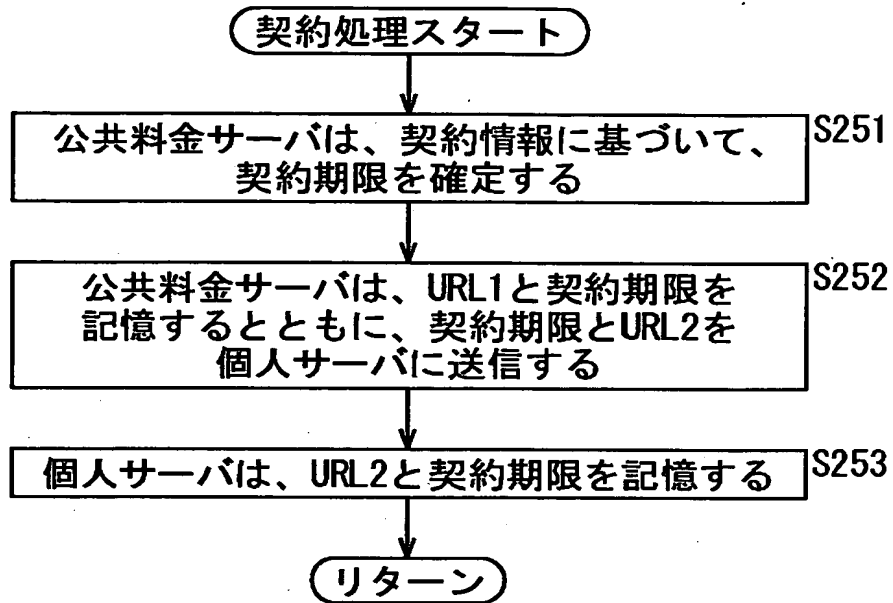
【図 35】



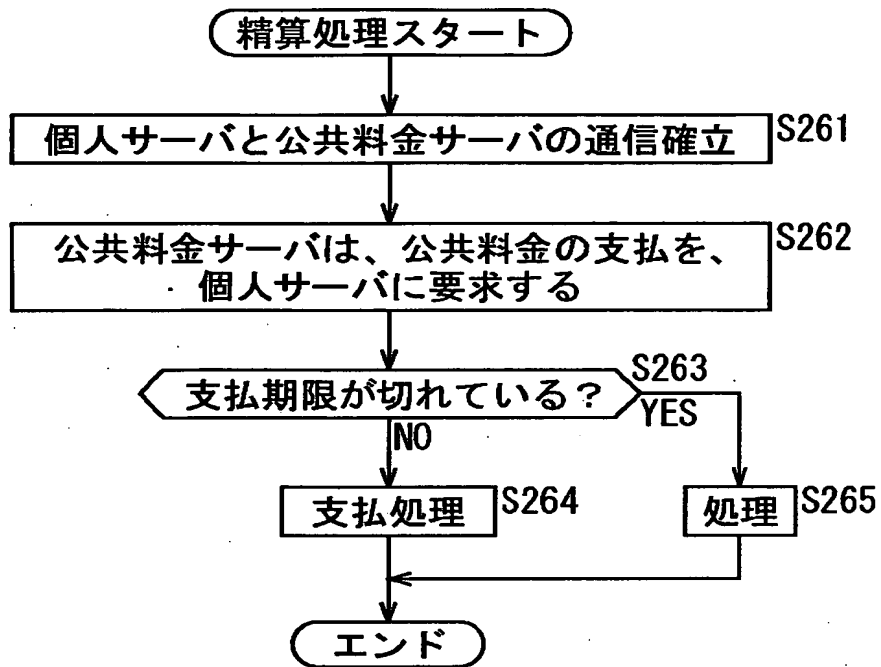
【図 3 6】



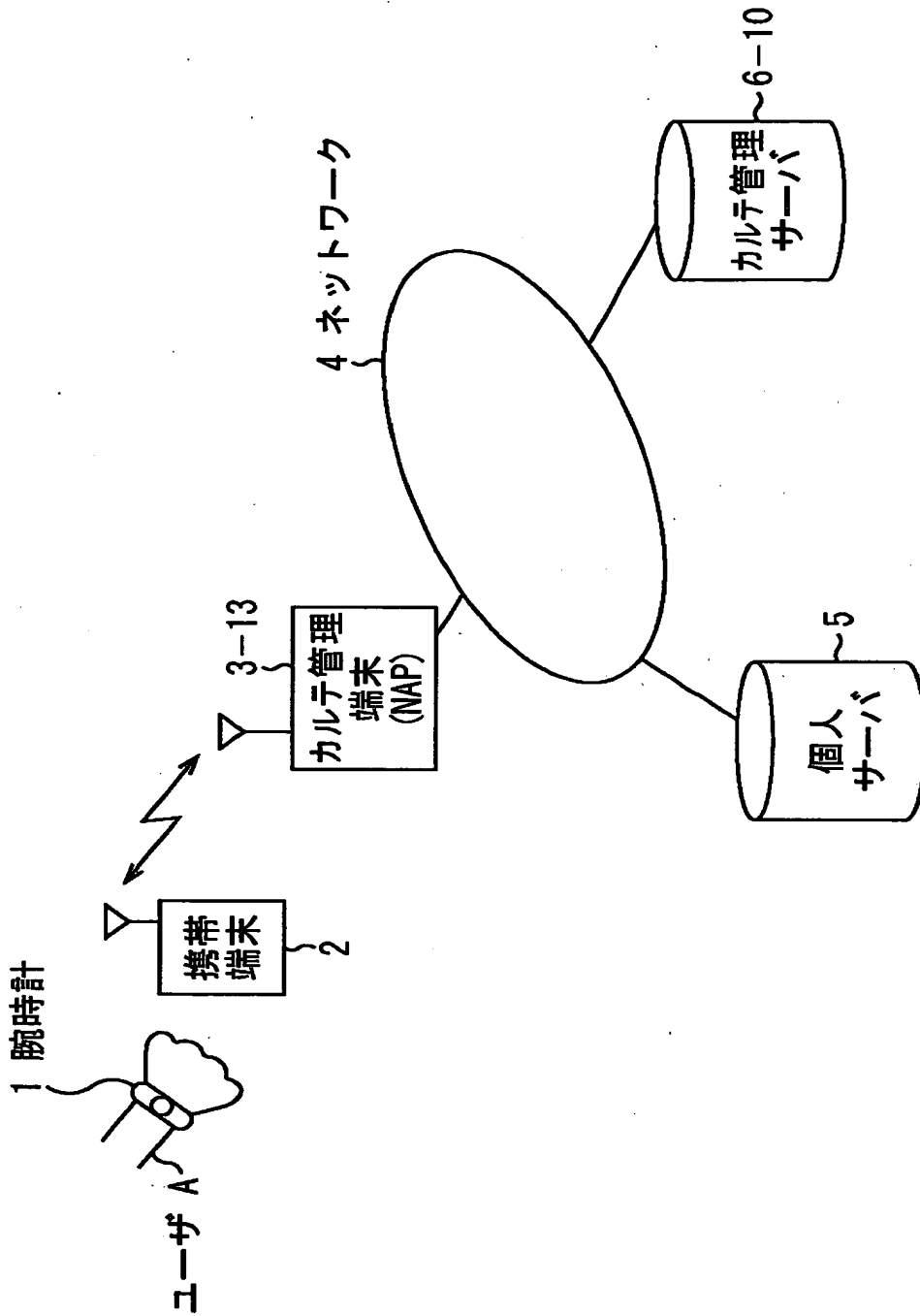
【図 3 7】



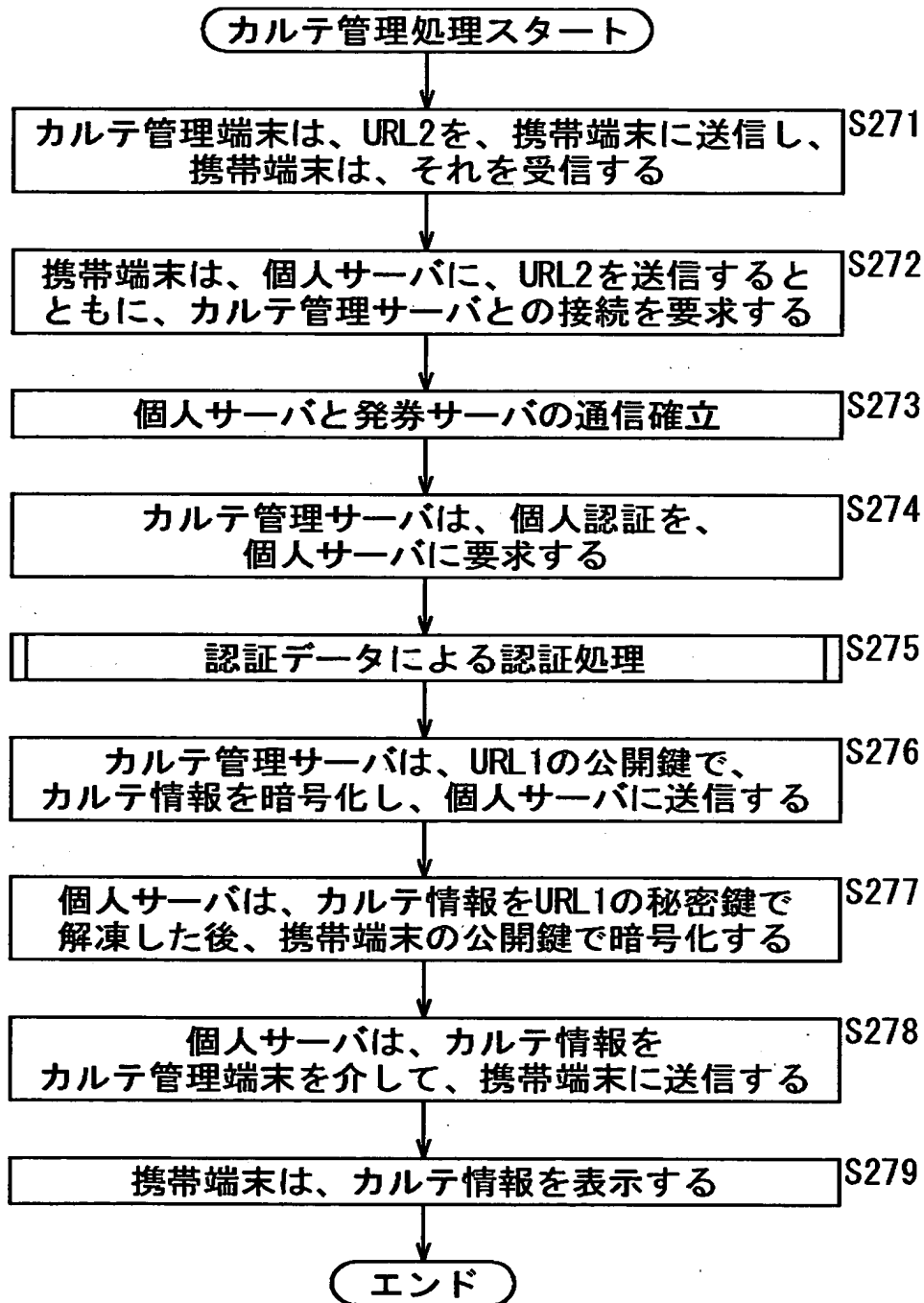
【図 3 8】



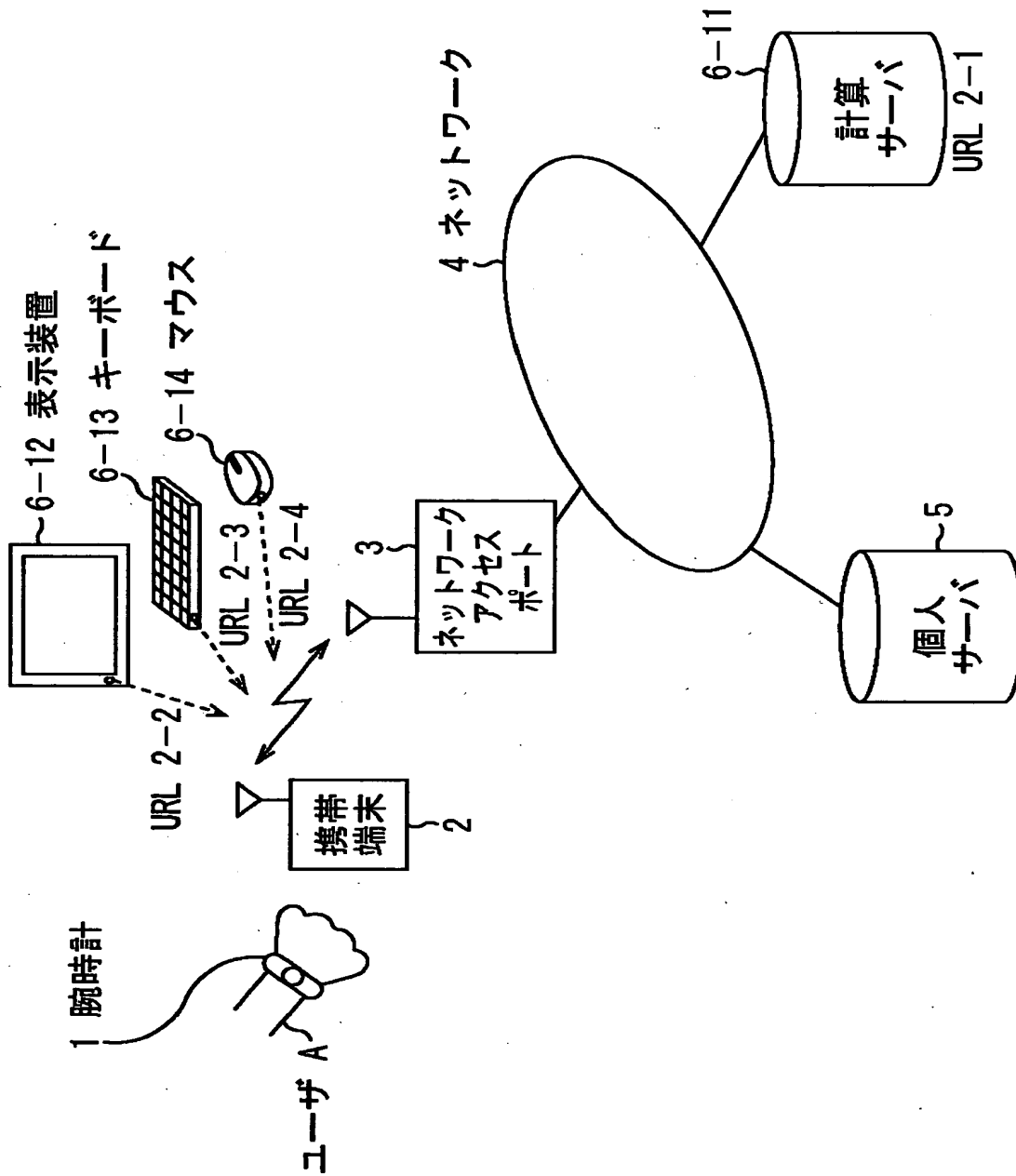
【図39】



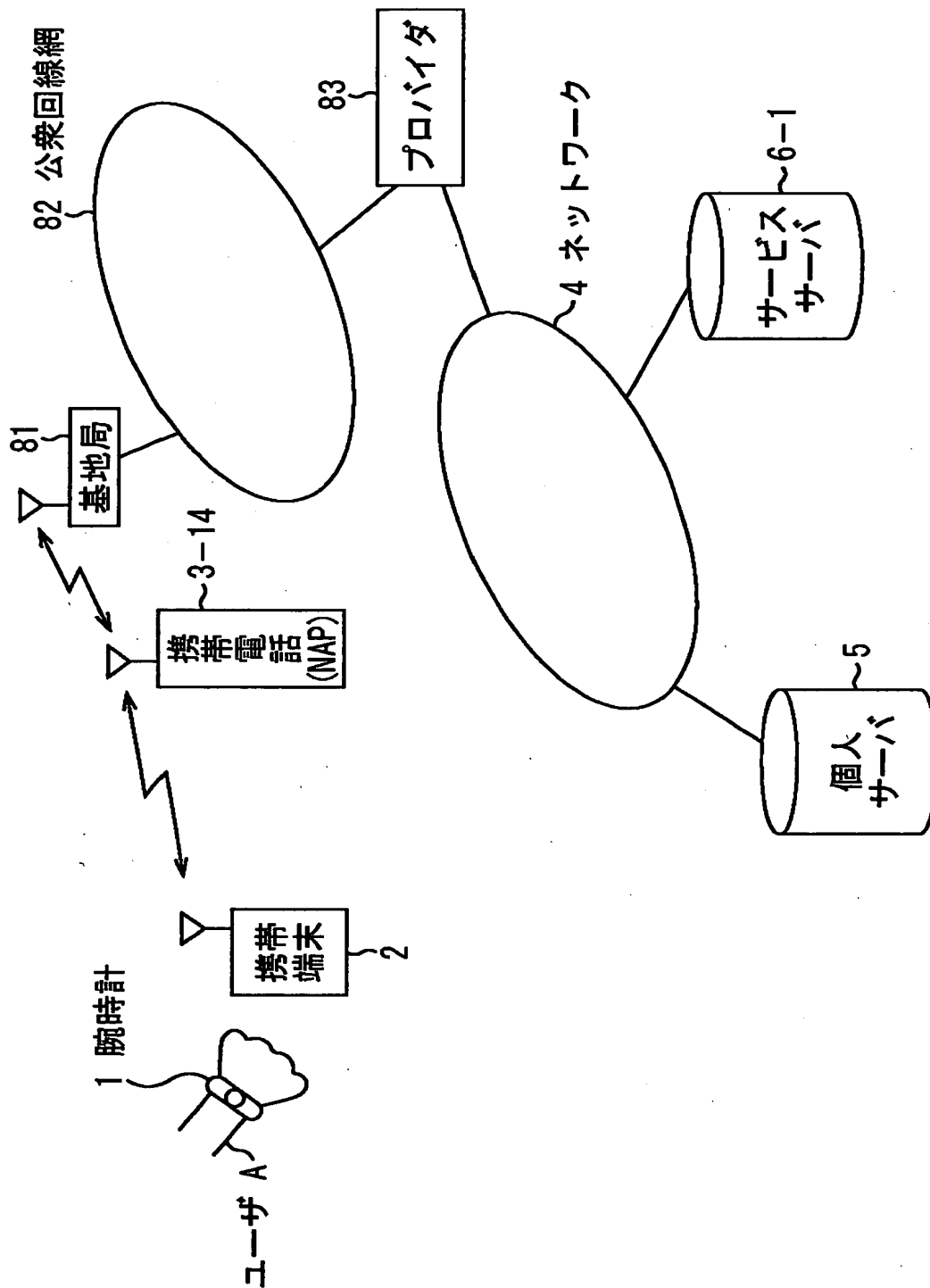
【図 4 0】



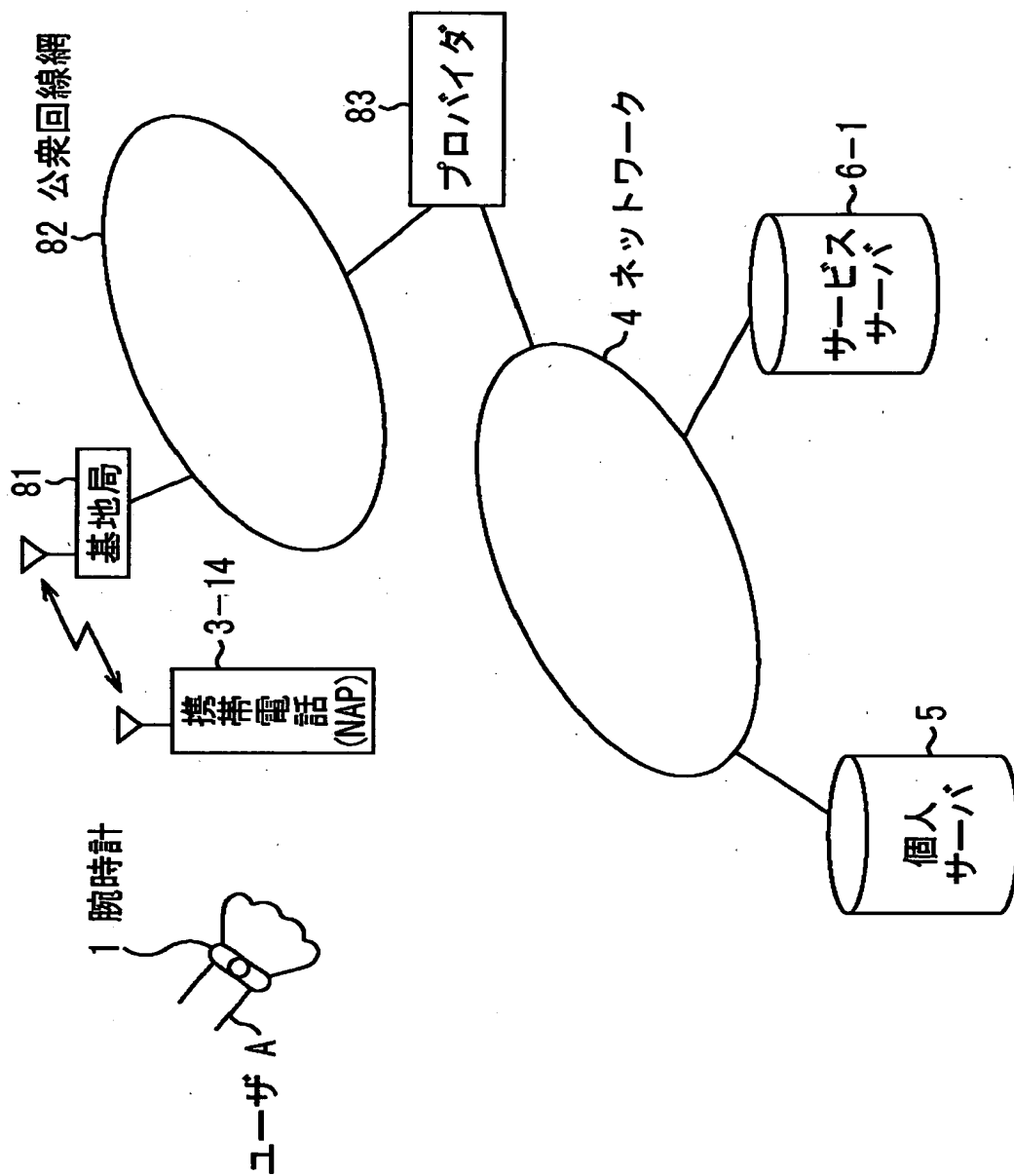
【図 4 1】



【図42】



【図43】



【書類名】 要約書

【要約】

【課題】 個人情報を保持しない携帯端末で、サービス提供システムを利用することができるようにする。

【解決手段】 腕時計 1 は、パスワードを発生する。携帯端末 2 は、個人サーバ 5 に記憶されているユーザ A の個人情報を指定する URL 1 を記憶しており、その URL 1 を、精算装置 3 - 1 に送信する。精算装置 3 - 1 は、携帯端末 2 に対するネットワークアクセスポートとしての役割を果たす。個人サーバ 5 は、URL 1 により特定される、ユーザ A の個人データを管理するサーバであり、ネットワーク 4 を介して、精算装置 3 - 1 やサービスサーバ 6 - 1 と通信する。サービスサーバ 6 - 1 は、URL 2 により特定される処理をサーバである。サービスサーバ 6 - 1 が、その処理を、ネットワーク 4 を介して、精算装置 3 - 1 や個人サーバ 5 と通信して実行する。これにより、ユーザ A は、各種サービスの提供を受けることができる。

【選択図】 図 1

出 願 人 履 歴 情 報

識別番号 [000002185]

1. 変更年月日	1990年 8月30日
[変更理由]	新規登録
住 所	東京都品川区北品川6丁目7番35号
氏 名	ソニー株式会社



Creation date: 09-10-2004
Indexing Officer: TBUI3 - TAI BUI
Team: OIPEBackFileIndexing
Dossier: 10039894

Legal Date: 05-14-2002

No.	Doccode	Number of pages
1	C.AD	1

Total number of pages: 1

Remarks:

Order of re-scan issued on